SMART LIVING

SECURITY SYSTEMS

Certified by
IMQ - Security systems
CEI 79-2
EN 50131-3
EN 50131-6
T014

GameOver

USER'S

MANUAL

inim®
ELECTRONICS

Warranty

INIM Electronics s.r.l. (Seller, Our, Us,) warrants the original purchaser that this product shall be free from defects in materials and workmanship under normal use for a period of 24 months. As INIM Electronics s.r.l. does not install this product directly, and due to the possibility that it may be used with other equipment not approved by Us; INIM Electronics s.r.l. does not warrant against loss of quality, degradation of performance of this product or actual damage that results from the use of products, parts or other replaceable items (such as consumables) that are neither made nor recommended by INIM Electronics. Seller obligation and liability under this warranty is expressly limited to repairing or replacing, at Seller's option, any product not meeting the specifications. In no event shall INIM Electronics s.r.l. be liable to the purchaser or any other person for any loss or damage whether direct ot indirect or consequential or incidental, including without limitation, any damages for lost profits, stolen goods, or claims by any other party caused by defective products or otherwise arising from the incorrect or otherwise improper installation or use of this product.

This warranty applies only to defects in parts and workmanship relating to normal use. It does not cover:

- damage arising from improper maintenance or negligence
- damage caused by fire, flood, wind or lightning
- vandalism
- fair wear and tear

INIM Electronics s.r.l. shall, at its option, repair or replace any defective products. Improper use, that is, use for purposes other than those mentioned in this manual will void the warranty. Contact Our authorized dealer, or visit our website for further information regarding this warranty.

Limited Warranty

INIM Electronics s.r.l. shall not be liable to the purchaser or any other person for damage arising from improper storage, handling or use of this product.

Installation of this Product must be carried out by qualified persons appointed by INIM Electronics. Installation of this Product must be carried out in accordance with Our instructions in the product manual.

Copyright

The information contained in this document is the sole property of INIM Electronics s.r.l. No part may be copied without written authorization from INIM Electronics s.r.l.

All rights reserved.

European Directive compliance

Hereby INIM Electronics s.r.l. declares that the SmartLiving series of intrusion-control panels, the Air2 series of devices and the SmartLink product are in compliance with the essential requirements and other relevant provisions of Directive 1999/5/CE.

Moreover, INIM Electronics s.r.l. also declares that all other devices mentioned in this manual are in compliance with the essential requirements and other relevant provisions of Directive 2004/108/CE.

The full declarations of conformity can be found at URL: www.inim.biz/dc.html.

State-of-the-art Installations (DM 37/08)

The devices described in this manual, in accordance with the settings selected during the installation phase and the following illustrated guidelines are, alternatively, in compliance with the the Italian Normative CEI 79-2:1998+Ab:2000 performance level 2 or European Normative CEI EN 50131-3:2009 (in reference to Control and indicating equipment - intrusion control panels) and CEI EN 50131-6:2008 (in reference to Power supplies) security grade 2.

In support of research, development, installation, testing, commissioning and maintenance of intrusion alarm systems installed in buildings please refer to the following normative documents:

CEI 79-3 e CEI CLC/TS 50131-7.

When installing INIM systems, it is up to the installer company to install systems equipped with Normative CEI 79-2 compliant devices rather than devices compliant with European Normatives series EN50131 within and not over the DOWs summarized in amendment CEI 79-2;V1:2010.

Table of contents

Warranty . . . 2
Limited Warranty . . . 2
Copyright . . . 2
European Directive compliance. . . . 2
State-of-the-art Installations (DM 37/08) . . . 2
Table of contents . . . 3

Chapter 1 General information . . . 5
1-1 Manufacturer's details . . . 5
1-2 Description of the product and various models . . . 5
1-3 Environmental Conditions . . . 6
1-4 Products certified and conforming to directives . . . 6
1-5 Manuals . . . 7
1-6 Operator Qualifications . . . 7
1-7 Access Levels . . . 7
1-8 Conventions – Glossary . . . 7

Chapter 2 The SmartLiving System . . . 8
2-1 Introduction . . . 8
2-2 The technologies . . . 9
2-3 Keypads . . . 9
2-4 Reader - nBy . . . 14
2-5 User Codes . . . 15
2-6 Keys . . . 16
2-7 Multi-system access . . . 17
2-8 Telephone functions . . . 18
2-9 WEB / e-mail functions . . . 18
2-10 Arming scenarios . . . 18

Chapter 3 Shortcuts . . . 19
3-1 Keypad shortcuts . . . 19
3-2 Shortcut with code . . . 20
3-3 Key and Reader shortcuts . . . 20
3-4 Shortcut list . . . 21

Chapter 4 Voice functions . . . 22

Chapter 5 Using the system . . . 23
5-1 Managing alarms . . . 23
5-2 Arming and disarming partitions . . . 24
5-3 Voice functions and Intercom (JOY/MAX only) . . . 26
5-4 Activations . . . 26
5-5 View . . . 28
5-6 Activating/Deactivating outputs . . . 30
5-7 Change date and time . . . 31
5-8 Keypad settings . . . 31
5-9 Change PIN . . . 32

5-10 Change telephone numbers 32
5-11 Teleservice request 33
5-12 Overtime request 33
5-13 Thermostat (JOY/MAX keypads only) 34
5-14 Listen-in 35
5-15 Partition status enquiry 35
5-16 Commands over-the-phone 35
5-17 Using the SmartLAN/G 37

Appendix A Technical terminology and Glossary 39

Appendix B Shortcuts at default 43

Appendix C Fault signals 44

Notes 45

Chapter 1

GENERAL INFORMATION

Manufacturer's details 1-1

Manufacturer: INIM Electronics s.r.l.
Production plant: Via Fosso Antico - Centobuchi
63076 Monteprandone (AP) - Italy
Tel: +39 0735 705007
Fax: +39 0735 704912
e-mail: info@inim.biz
Web: www.inim.biz

Any persons authorized by the manufacturer to repair or replace the parts of this system, hold authorization to work on INIM Electronics brand devices only.

Description of the product and various models 1-2

Description: Intrusion control panel
Models: SmartLiving 505
SmartLiving 515
SmartLiving 1050
SmartLiving 1050L
SmartLiving 10100L
Applied Normative: CEI 79-2:1998+Ab:2000, CEI EN 50131-3:2009 and CEI EN 50131-6:2008
Certification agency: IMQ Security Systems
Security rating: 2

The following table describes the main features of the various models of the SmartLiving series:

Table 1: **Control panel - Main Features**

SmartLiving intrusion control panels	505	515	1050	1050L	10100L
Total terminals	5	15	50		100
Terminals on panel	5		10		
Terminals on panel configurable as inputs	5		10		
Terminals on panel configurable as Rollerblind/Shock	2				
Terminals on panel configurable as outputs	0		5		
Total zones	10	30	100		200
Relay outputs on panel motherboard	1				
Open-collector outputs on panel motherboard	2 (150mA)		2 (500mA)		
Partitions	5		10		15
Keypads (JOY, nCode/G, Concept/G)	5		10		15
nBy Readers	10		20		30
Digital keys and keyfobs	50		100		150
Possible key-code combinations	4294967296				
Codes	30		50		100
Scenarios	30				
Timer	10				20
Recordable Events	500				1000

Environmental Conditions 1-3

The JOY/GR, JOY/MAX, nCode/G, Concept/G, IB100, FLEX5, Nexus and nBy/X peripheral devices are for indoor installation only and operate best under the following environmental conditions:

- **Temperature**: from -10° to +40°C
- **Maximum humidity**: 75% (without condensation)
- **Environmental class**: II

The nBy/S reader is suitable for indoor or outdoor installation, and operates best under the following conditions:

- **Temperature**: from -25° to +70°C
- **Maximum humidity**: 93% (without condensation)
- **Protection grade**: IP 34
- **Environmental class**: IV

Products certified and conforming to directives 1-4

When duly programmed, the SmartLiving intrusion control panel and the devices described in this manual have been certified by the IMQ - Security Systems agency as compliant with CEI 79-2:1998+Ab:2000, CEI EN 50131-3:2009 and CEI EN 50131-6:2008.

The Control panel enclosure houses the following certified devices:

- INIM Electronics switching-power supply
- Mother board (IN082 or IN088)
- SmartLogos30M voice board (accessory item)
- FLEX5/U input/output expansion board (accessory item)
- AUXREL32 relay board (accessory item)
- SmartLAN/SI and SmartLAN/G LAN interface boards (accessory items)
- IB100/RU BUS isolator board (accessory item)
- ProbeTH thermal-probe kit for battery-charge optimization (accessory item)
- TamperNO tamper-protection kit (accessory item)
- Backup battery, 12 V @ 17 Ah
- Motherboard (IN082 and IN088) integrated Type B notification apparatus

The control panel compliancy is also guaranteed when connected to the following certified devices:

- FLEX5/P input/output expansion boards
- Joy/MAX, Joy/GR, Concept/G, nCode/G keypads
- nBy/S outdoor-mount proximity readers
- nBy/X universal-mount proximity readers
- IB100/RP BUS isolator
- Self-powered IB100/A BUS isolator
- nCard access-control card for proximity readers
- nTag access-control tag for proximity readers

Compliancy is not guaranteed when the control panel is connected to the following uncertified devices:

- SmartLink/GWB GSM interface with 12V @ 1.2 Ah battery
- BUS-connected Nexus interface
- BUS connectable Ivy-B, Ivy-BF, Ivy-BM, and Ivy-BFM self-powered sounderflashers for outdoor installation
- Wireless devices such as: AIR2, AIR2-BS100 (transceivers), Air2-IR100 (PIR detectors), Air2-MC100 (magnetic contacts), Air2-KF100 (access-control keyfobs)
- SmartModem100 Teleservice modem

TYPE B NOTIFICATION APPARATUS

ATS2 notification apparatus (refer to EN50131-1:2008-02, paragraph 8.6 Notification, Table 10, page 46, Grade 2 and EN50136) characterized by:

- Transmission time - classification D2 (60 seconds)
- Transmission time - max. values M2 (120 seconds)
- Classification time - classification T2 (25 hours)
- S0 Substitution security (no detection of device substitution)
- I0 Information security (no detection of message substitution)

Manuals 1-5

Installation Manual 1-5-1

The installer should read carefully through the Installation Manual and should be familiar with all the components and the operating procedures of the SmartLiving system. In order to provide adequate protection, the installer must adhere to all the manufacturer's guidelines relating to the active and passive security devices of this system. It is the installer's responsibility to inform the system users that, regardless of its capabilities, an intrusion alarm system is not a substitute for the necessary precautions building occupants must take to prevent intrusion.

User's Manual (this manual) 1-5-2

DCMUINE0SLIVINGE **MANUAL CODE**

4.00 **VERSION**

The installer should read carefully through the User's Manual (supplied with each control panel). Once the system has been installed, the installer must ensure that the User's Manual is available to the users for consultation, and that they fully understand how the system works and are aware of all the functions, settings and procedures.

Operator Qualifications 1-6

Installer 1-6-1

The installer is the person (or group of persons) who sets up and programs the entire security system in accordance with the purchaser's requirements and in respect of the safety laws in force. As the only individual in contact with system users, it is the installer's responsibility to instruct them on how to use the security system properly.

Under normal circumstances, the installer is not allowed to arm/disarm the system without previous authorization from the user. All the system partitions must be disarmed before accessing the parameter programming phase.

User 1-6-2

The users are the occupants of the building where this intrusion control panel is installed. Only authorized users can operate the system.

The most common operations can be carried out without code/key verification. This method must be expressly requested by the main user, as it considerably lowers the security level of the system and may cause false alarms, accidental arm/disarm operations, etc.

Access Levels 1-7

The normative defines the following system-access levels, regardless of system-access limitations:

- **Level 1** - access by any person (e.g. passer-by)
- **Level 2** - user access
- **Level 3** - installer or maintenance operator access (authorized by user - level 2)
- **Level 4** - manufacturer access

Conventions – Glossary 1-8

In order to help users understand the terminology utilized in this manual and improve your knowledge of this system and its operating procedures, read carefully through the Technical Terminology – Glossary (refer to *Appendix A, Technical terminology and Glossary*).

The appendix contains the definitions of technical terms commonly used in the field of security, therefore, relevant to the SmartLiving system.

Chapter 2

THE SMARTLIVING SYSTEM

Introduction 2-1

INIM Electronics wishes to thank you for choosing this SmartLiving intrusion control system. Its advanced technology and user-friendly operations provide an extremely high level of protection combined with ease-of use.

INIM Electronics recommends that all parts of this manual be read thoroughly before starting up SmartLiving system. Once you have become accustomed to the day-to-day operations, your installer will explain and if required, program the advanced functions provided by the system.

A typical system comprises:

- SmartLiving control panel
- intrusion detection devices (PIR or microwave detectors, magnetic contacts, linear beam detectors, etc.)
- system control peripherals: proximity readers, keypads
- alarm signaling devices which generally signal the events detected by the system (sounders, flashers, etc.)

The keypad (Joy/GR, Joy/MAX, nCode/G or Concept/G) is an extremely flexible peripheral device which allows you to manage the system with ease. The graphic display provides all the information necessary for fast understanding of the system status, and the steps necessary to take in the event of an alarm. All users have PINs which allow them to access and control the system in accordance with their permitted access level.

Advanced voice technology guides you through the operations by means of clear voice prompts which explain the operations you must undertake.

nBy readers (2 versions available: nBy/S wall-mount and By/X flush-mount) allow you to access and control the system. Although these devices are not as flexible as keypads, they provide a quick and easy way of carrying out day-to-day operations such as arming and disarming the system. Authorized digital-key users can operate the system in accordance with their programmed access level (enabled functions, etc.) by holding the key in front of the proximity key reader.

All SmartLiving control panels are capable of managing INIM's "Air2" two-way wireless system. This system integrates wireless devices (detectors, keyfobs, etc.) into the hardwired environment.

SmartLiving control panels are capable of managing various event types (alarms, faults, tamper, code/key identification, arm/disarm operations, etc.) and event-response actions (audible/visual signaling, telephone calls, SMS text messages over the GSM network and, with the addition of the optional SmartLan/G board, e-mails with attachments). The calls can be:

1. report calls to alarm receiving centres - via the most widely used reporting protocols.
2. voice calls to contact numbers - using advanced voice technology to inform contact persons of the active alarm condition.

Events can also be announced on JOY/MAX keypads.

The SmartLiving intrusion control panel also provides automatic features, such as:

- arm and disarm operations set up on a weekly basis
- simple yet useful access-control functions which allow the system to deny access to specific keys/codes at certain times
- pre-set activation/deactivation of household devices (building automation) such as courtesy lights
- other similar automatic facilities.

The technologies 2-2

Expertise in the arena of total security and a commitment to precision and high quality allow INIM's R & D professionals to deliver excellence in design technology and dependability through time.

EASY4U 2-2-1

This user-friendly tool provides an interesting array of graphic features and functions. All SmartLiving intrusion control panels are controlled by keypads equipped with 96x32 pixel graphic displays. The four-line alphanumeric display screen (16 characters per line) can be edited or used to view the icons associated with various customized user-operations. The keypad shortcuts allow time-consuming sequences to be transformed into simple keystroke actions. In this way, frequently-used or repetitive sequences of keystrokes can be eliminated. The shortcuts can be used for a variety of tasks and make operations less tedious and less error-prone. The use of customizable graphic-objects, which indicate the system status, helps users to understand what is happening on the system..

Besides accepting various commands (Away Arm, Stay Arm, Disarm, etc.), the nBy reader also allows users to manage the "shortcuts" programmed on the keypad.

The JOY/MAX keypad provides a built-in nBy key reader.

VOIB 2-2-2

This is an acronym for **V**oice **O**ver **I**nim-**B**us. VOIB technology allows the system to manage end-to-end digitized voice transmissions at extremely high-speed over the IBUS. Voice transmissions can be carried to all points of the IBUS. The JOY/MAX keypad provides a built-in microphone and speaker for message recording and playback. The 30 minute capacity voice board allows each event to be associated with a message. Voice digitizing and compression allow the signal to be transmitted in data packets over the bus to recipient keypads where it is announced. Voice digitizing and the characteristics of the I-BUS allow end-to-end "noise-immune" voice transmissions without the need of any additional wiring.

Keypads 2-3

The keypad allow users to manage all aspects of the security system. SmartLiving control panels support JOY/GR, JOY/MAX, nCode/G and Concept/G keypads. The features of these keypads are described in the following table:

Table 2: **Keypads - functions**

	JOY/MAX	JOY/GR	nCode/G	Concept/G
Graphic display	Yes			
Keys	23 (in soft rubber)			23 (touch)
Signaling LEDs	4			
Buzzer	Yes			
Terminals	2		1	
Microphone	Yes	No		
Loudspeaker	Yes	No		
Built-in proximity reader	Yes	No		
Temperature sensor	Yes	No		
Backlight activated by proximity sensor	No			Yes
Block keypad	No			Yes

The various keypad models provide diverse functions, casings and key access. Joy keypads have a flip which protects the keys, whereas, the keys of the nCode/G and Concept/G keypads are on view. The Concept/G is a touch keypad.

The keypad is the device that allows authorized code users to control the entire system or specific partitions. However, system control can be extended to other building occupants who do not hold a valid code.

The SmartLiving intrusion control panel offers an array of innovative features. In addition to the traditional User menu (accessed by means of user-code entry),

this system provides a series of shortcuts" (refer to "Shortcuts" in Appendix) associated with keys F1 Fn F2 F3 F4 .

Generally, intrusion control panels do not allow access to the system via keypad without code entry. However, by means of the customized (personal) shortcuts associated with keys F1 Fn, ..., F4 it is possible to enable building occupants to access and operate the system without code entry.

The installer must program the shortcuts to suit user requirements and explain how they are used. For example, it may be useful to allow all the building occupants to arm the system without code entry, as this operation increases the level of system security. However, operations which lower the level of system security should be reserved for code users only. Under normal circumstances, operations which increase system security can be allowed without valid-code entry whereas, operations which lower system security (Disarm, Delete Alarm/Tamper memory, Deactivate Alarm/Tamper outputs) should be allowed only after valid-code entry.

Each keypad is assigned (by the installer) to the partitions it controls.

JOY/MAX keypads also provide a programmable chronothermostat function. This function allows you to set up zone management (one zone per keypad) of the heating/air-conditioning system.

The temperature is gauged by a built-in temperature sensor. The hysteresis is fixed at 0.4°C.

The Concept/G keypad provides a further two options relating to direct user access.

A special feature allows activation of the backlight of the display and keys when users approach the keypad. This is achieved through a proximity sensor which can be activated by pressing keys 1 and * simultaneously and deactivated by pressing 1 and #.

The other option, block/unblock keypad, can be achieved by pressing key * for 3 seconds. If the block keypad option is enabled, the display will show the icon opposite.

Display - description 2-3-1

The brightness and contrast of the backlit-graphic LCD (96 x 32 pixel) can be adjusted by way of the respective options on the User Menu (refer to paragraph *5-8 Keypad settings*).

The first line of the display shows the date and time. If you are using a JOY/MAX keypad, the date and room temperature will alternate on the screen every 3 seconds.

The left side of the second line shows the characters that indicate the current status of the partitions the keypad is assigned to:

- **D** = partition disarmed
- **A** = partition armed in Away mode (interior and perimeter zones armed)
- **S** = partition armed in Stay mode (perimeter zones armed)
- **I** = partition armed in Instant mode (perimeter zones armed with no delay)
- **-** = partition does not belong to the keypad

The displays of the SmartLiving 505 and 515 models show 5 characters indicating the status of partitions 1 to 5 (both models have 5 partitions).

The displays of the SmartLiving 1050 and 1050L models show 10 characters indicating the status of partitions 1 to10 (both models have 10 partitions).

The display of the SmartLiving 10100L model, alternates at 3 second intervals, between 10 characters indicating the status of partitions 1 to 10 and 5 characters indicating the status of partitions 11 to 15 (the 10100L model has 15 partitions).

If a partition has memory of an alarm or tamper condition, the character that represents the partition concerned will blink.

The right side of the second line shows several icons which provide visual information regarding the system.

Table 3: **The icons (shown on the second line of the display)**

Icon	Name	Not present	On solid	Blinking or interchanging icons
	Telephone line		Telephone line busy	(Icon blinking) Telephone line down
	Peripheral tamper	All peripherals are properly placed and all enclosures covers are closed.	At least one peripheral (keypad, reader, expansion) is in tamper status (enclosure open or device dislodged).	(Interchanging icon) All peripherals are properly placed and all enclosure covers are closed, however, tamper has been detected and cleared (Tamper memory).
	Peripheral Loss	All the peripherals in the system configuration are responding properly (Present).	At least one peripheral (keypad, reader, expansion) is not responding properly.	(Interchanging icon) All the peripherals in the system configuration are responding properly, however, loss of a peripheral has been detected and cleared (Peripheral Loss memory).
	Answerphone	Answerphone function disabled	Answerphone function enabled	
	Teleservice	Teleservice disabled	Teleservice enabled	
	Key			(Icon blinking) False key
	Control panel Tamper	The Control panel is properly placed and the enclosure is closed.	The Control panel is in tamper status (enclosure open or device dislodged).	(Interchanging icon) The Control panel is properly placed and the enclosure is closed, however, panel tamper has been detected and cleared (Panel tamper memory).
	Thermostat: Winter mode	The thermostat option is disabled.	The keypad thermostat option is enabled in Winter mode (Heating).	
	Thermostat: Summer mode		The keypad thermostat option is enabled in Summer mode (Air-conditioning).	
	Thermostat: Heating/Air-conditioning	Heating/Air-conditioning Off.	Heating/Air-conditioning On.	

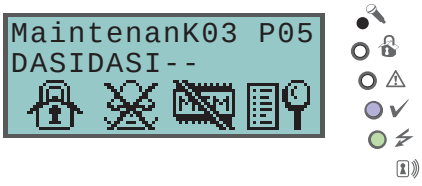
Note

If duly programmed by the installer, the icon will not be shown when Teleservice is enabled.

The remaining section of the display (that is, the third and fourth line) is occupied by the icons which correspond to the Shortcuts associated with keys F1 Fn, ..., F4 POL. If the function keys have not been associated with shortcuts, the third and fourth line will be empty.

2-3-2 Display - standby status

A) If the control panel is in Maintenance status, the first line on the screen will show the string indicated in the figure. The characters "K03" indicate the address assigned to the keypad (in the example, the keypad is at address 3). If you are using a Joy/MAX keypad, the string will also show "P05", which is the address assigned to the built-in proximity reader (in the example, the reader is at address 5).



B) If any of the keypad partitions has Alarm or Tamper memory, the first line of the screen will flash the descriptions of the zones concerned every 3 seconds. In the event of Alarm or Tamper memory, the red LED on the keypad and the characters corresponding to the partitions concerned will blink.

C) If the control panel is in Maintenance status and any of the keypad partitions has memory of an Alarm or Tamper condition, the first line on the screen will show the strings described in points A) and B).

D) If the "View open zones of disarmed partitions" option is enabled, the first line on the screen will flash (approximately every 3 seconds) the descriptions of any zones which are not-in-standby status when the keypad partitions disarm. Any auto-bypassable zones will be shown in white on black background.

Note

Case D is discernible from case B in the fact that in case B, the red LED on the keypad blinks.
Case D is viewable only when the conditions of cases A, B and C are not present.

Using the keypad 2-3-3

The following section describes how the keys are normally used. Some of the keys may have specific functions which will be indicated when necessary.

Table 4: **The keys**

Keys	Name	Typical application
1 ., 2 abc, 3 def, 4 ghi, 5 jkl, 6 mno, 7 pqrs, 8 tuv, 9 wxyz, 0 ␣	**Number keys**	Used to type in User PINs
OK	**OK**	Confirms the selected item (parameter, etc.)
	UP, DOWN	Navigate through the menu lists or adjust keypad volume
	LEFT, RIGHT	Scroll along the data rows (for example, partitions in the events log, etc.).
C	**C**	Steps back on the open menu without changing the selected item (parameter, etc.) or, after entering a User PIN and pressing OK, runs through the 3 User-menu templates (refer to paragraph *2-5 User Codes*) each time it is pressed.
Esc	**ESC**	Exits the User menu without changing the selected item (parameter, etc.).
*	**ENABLE**	Enables options (refer to paragraph *5-4 Activations*)
#	**DISABLE**	Disables options
F1 Fn, F2, F3, F4	**F1, F2, F3, F4 or function keys**	Activate the shortcuts which correspond to the associated icons. Can be used also as Emergency keys (refer to paragraph *2-3-4 Emergency keys*).

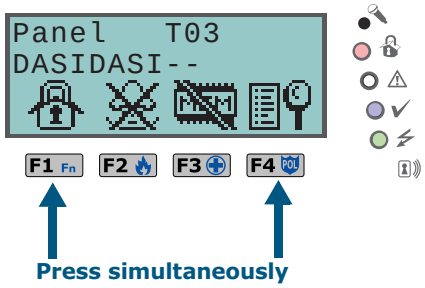
Emergency keys 2-3-4

This control panel provides 3 "key-duos" for Emergency Calls which can be activated by pressing the respective keys on any of the system keypads:

1. F1 Fn + F2 = Fire Emergency
2. F1 Fn + F3 = Ambulance Emergency
3. F1 Fn + F4 = Police Emergency

Utilization of any of the "key-duos" will generate the respective events and actions (e.g. activation of outputs and calls).

To activate an emergency call, press simultaneously and hold keys F1 Fn + F2, or F1 Fn + F3, or F1 Fn + F4 for at least 3 seconds until the selected emergency call is confirmed by a beep.



Note

If any two function keys are pressed at the same time, the functions relating to the icons associated with the keys will not be activated.

Visual signals on the keypad LEDs 2-3-5

The following table describes the visual signals on the keypad LEDs.

Table 5: **Keypad LEDs**

LED	Red	Yellow	Blue	Green
OFF (no light)	All the keypad partitions are disarmed.	No faults present.	Open zones on the keypad partitions.	Primary power failure (230V a.c.)
ON (Solid)	At least one of the keypad partitions is armed.	At least one fault has been detected.	All the zones on the keypad partitions are in standby status: Ready to arm.	Primary power OK (230V a.c.)
Slow blinking (ON: 0.5sec OFF: 0.5sec)	All the keypad partitions are disarmed. Memory of alarm/ tamper on at least one of the keypad partitions or memory of a system alarm.	No faults present. At least one of the zones belonging to the keypad partitions is either disabled (inhibited) or is in Test status	All the zones belonging to the keypad partitions are in standby status. (For JOY/MAX only: an unplayed voice message is present in the memo box).	
Fast blinking (ON: 0.15sec OFF: 0.15sec)	At least one keypad-partition is armed. Memory of alarm/ tamper on at least one of the keypad partitions or memory of a system alarm.	At least one fault is active and at least one zone belonging to the keypad partitions is either disabled (inhibited) or is in Test status.	Open zones on the keypad partitions. (For JOY/MAX only: an unplayed voice message is present in the memo box).	

The list of faults signaled on the yellow fault LED ⚠ can be found in the table in *Appendix C, Fault signals*.

Following is the list of events which cause the Red System Alarm LED to blink:

- Open panel tamper
- Dislodged panel tamper
- Expansion tamper
- Keypad Tamper
- Reader Tamper
- Expansion Loss
- Keypad Loss
- Reader Loss
- False key

If the "False key" event is configured as a "Silent event", the red LED will not blink.

"FALSE KEY"

If this option is enabled, the status of the partitions will be hidden. If a valid code is entered at a keypad, the real-time status will be indicated on the keypad concerned for 30 seconds. Additionally:

"50131STATHIDDEN"

- If the partitions are armed, the status of the system will be hidden from non-authorized users.
  - •• Red keypad LED Off
  - •• Yellow keypad LED Off
  - •• Green keypad LED On solid
  - •• Status icons not present
  - •• Alarm and Tamper memory hidden
  - •• If a particular event occurs more than 5 times when the partitions are armed, it will not be signaled as having occurred more than 5 times. This is due to the limitation placed on the counter of each event. The counters will reset to zero each time all the partitions are disarmed.
- If the partitions are DISARMED:
  - •• LEDs operating normally.
  - •• Status icons present
  - •• Alarm and Tamper memory visible

Signaling on the Buzzer 2-3-6

The buzzer signals the running Entry, Exit and Pre-arm times (refer to *Appendix A, Technical terminology and Glossary*) of enabled partitions.

Buzzer signal	Description
8 pulses with 5 second pause	Entry time
3 pulses with 5 second pause; 4 short pulses with 5 second pause during the final 20 seconds of the Exit Time	Exit time
1 pulse with 5 second pause	Pre-arm time

Emergency status 2-3-7

In the event of a keypad configuration or communication error between the system peripherals, the display will show one of the templates opposite.

If this occurs, you must contact your installer immediately and get the fault cleared.

```
  - JOY/MAX -
FW RELEASE  3.00
NO COMMUNICATION
K01 P14
```

```
  - JOY/MAX -
FW RELEASE  3.00
NOT ENROLLED
K01 P14
```

Reader - nBy 2-4

The SmartLiving intrusion control panel manages nBy/S and nBy/X readers and also JOY/MAX-keypad readers.

The proximity reader is the easiest way for users to interact with the SmartLiving intrusion control system.

The wall-mount nBy/S model (anchored by means of two screws) is IP34 rated and therefore suitable for outdoor use.

It is equipped with a buzzer and 4 LEDs:

- **F1**- Red
- **F2** - Blue
- **F3** - Green
- **F4** - Yellow

The Universal flush-mount nBy/X (**Patent Pending**) has been especially designed to integrate with all brands of cover plates.

It is equipped with 4 LEDs (red, blue, green and yellow).

Readers do not provide the same extent of system control as keypads, however, these devices are quick and easy-to-use and are extremely useful when carrying out day-to-day operations (arm/disarm partitions, etc.).

Readers are usually located near the main entry/exit points of the protected building. These devices allow system access to valid keys only. The system readers are capable of recognizing a large number of keys, each characterized by customized parameters.. Each reader is enabled to operate on specific partitions, whereas each key is enabled to operate only on the partitions the user is allowed to control. Therefore, if a key is held in the vicinity of a reader, it will be possible to control only the partitions which the two devices have in common.

Each reader can be programmed with up to 4 shortcuts (one per LED).

Each key can be programmed with up to 4 shortcuts.

Unlike most traditional readers (which generally carry out arm/disarm operations only), nBy readers also manage a series of useful shortcut commands. For example, it is possible to associate two shortcuts to the red and blue LEDs for arm and disarm operations, and a shortcut to the green LED for gate control, and yet another to the yellow LED for "Clear call queue" operations.

The buzzer signals the running Entry, Exit and Pre-arm time of the reader partitions (refer to paragraph *2-3-6 Signaling on the Buzzer*).

Signaling on the Reader LEDs 2-4-1

The LEDs have two distinct operating in modes:

1. When no key is present at the reader (refer to *Table 6: Reader LEDs with no key at reader*), the LEDs will indicate the current status of the associated shortcut.
2. When a key is present at the reader (refer to *Table 7: Reader LEDs with key at reader*), the LEDs will indicate (in rapid succession) the available shortcuts.

Table 6: **Reader LEDs with no key at reader**

LED	Red	Blue	Green	Yellow
OFF (All LEDs Off)	All the reader partitions are disarmed. No alarm/tamper memory on the reader partitions or system tamper memory.			
ON / OFF (in accordance with the associated shortcut)	The scenario associated with the arming-shortcut of the red LED is active/inactive. The output associated with the output-activation shortcut of the red LED is active/inactive. Faults are present/not present.	The scenario associated with the arming-shortcut of the blue LED is active/inactive. The output associated with the output-activation shortcut of the blue LED is active/inactive. Faults are present/not present.	The scenario associated with the arming-shortcut of the green LED is active/inactive. The output associated with the output-activation shortcut of the green LED is active/ inactive. Faults are present/not present.	The scenario associated with the arming-shortcut of the yellow LED is active/inactive. The output associated with the output-activation shortcut of the yellow LED is active/ inactive. Faults are present/not present.
Intermittent blinking (ON: 2.3sec OFF: 0.1sec)	At least one Reader-partition is armed.			
Slow blinking (ON: 0.5sec OFF: 0.5sec)	The reader partitions are disarmed. Alarm/tamper memory on at least one of the reader partitions, or system tamper memory.	The scenario associated with the last key used is active.		
Fast blinking (ON: 0.15sec OFF: 0.15sec)	At least one Reader-partition is armed. Alarm/tamper memory on at least one of the reader partitions, or system tamper memory.			

Table 7: **Reader LEDs with key at reader**

LED	Red	Blue	Green	Yellow
OFF (no light)	Request to arm ALL the partitions common to both the key and reader.			
ON (only one LED On)	Request to activate the shortcut associated with the red LED on the reader or the first shortcut of the key	Request to activate the shortcut associated with the blue LED on the reader or the second shortcut of the key	Request to activate the shortcut associated with the green LED on the reader or the third shortcut of the key	Request to activate the shortcut associated with the yellow LED on the reader or the fourth shortcut of the key
ON (All the LEDs On).	Request to activate the shortcut associated with the key.			
Fast blinking (ON: 0.15sec OFF: 0.15sec one LED only)	If the shortcut associated with the red LED is an arming operation, one of the partitions concerned is not-ready-to-arm due to zones which are not in standby status.	If the shortcut associated with the blue LED is an arming operation, one of the partitions concerned is not-ready-to-arm due to zones which are not in standby status.	If the shortcut associated with the green LED is an arming operation, one of the partitions concerned is not-ready-to-arm due to zones which are not in standby status.	If the shortcut associated with the yellow LED is an arming operation, one of the partitions concerned is not-ready-to-arm due to zones which are not in standby status.
Fast blinking (ON: 0.15sec OFF: 0.15sec ALL LEDs)	If the shortcut associated with the key is an arming operation, one of the partitions concerned is not-ready-to-arm due to zones which are not in standby status.			

Note

If a key is present, all operations (arm, disarm, etc.) will apply only to the partitions common to both the key and reader.

"50131READERLEDOFF"

If this option is enabled and there are no keys present at the reader, the reader LEDs will be Off.

User Codes 2-5

Each User Code comprises a PIN for identification purposes and a group of parameters which determine its rank in the system code hierarchy and the operations the user is entitled to perform.

The PIN is made up of 4, 5 or 6 digits that the user must enter in order to allow identification.

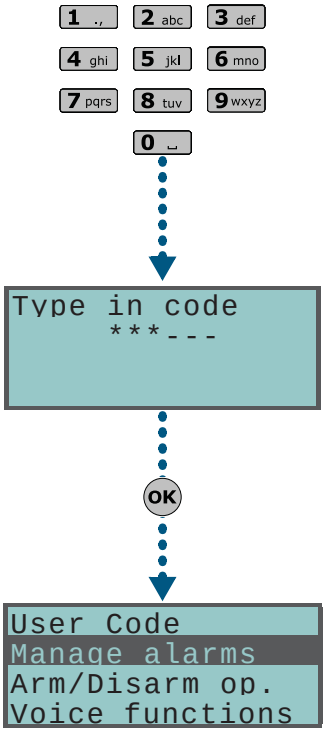
The PIN of the only user code enabled at default is 0001. The PINs of the successive codes are 0002, 0003, etc.

Note

The installer is allowed to change User code PINs. The installer provides the system users with default user PINs which they must change immediately to PIN codes of their choice.

Each user code is characterized by the following parameters, programmed by the installer in accordance with specific user rank.

- **Partitions** - User codes can control only the partitions they are assigned to. If a user code is entered at a keypad, the user can control only the partitions which are common to both the code and keypad concerned. For example, if a code enabled on partitions 1, 2, 3, 4 and 5 is entered at a keypad which enabled on partitions 4, 5, 6 and 7, it will be able to operate on partitions 4 and 5 only.
- **User Code Type** - Rank There are two user code types (ranks), "Main User" and "User". "Main User" codes can disable ordinary "User" codes and change their PINs. However, a "Main User" code cannot be used to disable another "Main User" code or change its PIN. "User" codes can change their own PINs only.
- **User Menu Access mode** Each User code can access its customized menu in 3 different ways (refer to paragraph *2-5-1 Accessing the User Menu*).
- **Commands over-the-phone** This option enables access to the system via remote telephone. If this option is enabled, the User can send commands to the control panel over-the-phone. Commands can be sent during calls to/from the control panel. After a valid PIN entry on the telephone keypad the user can activate specific shortcuts (refer to *Chapter 3 - Shortcuts*). This method of entering commands will affect the code partitions only.
- **Timer Restriction** If a code is associated with one of the timers, it will be able to operate the system only when the Timer is On.
- **Group of outputs which can be activated/deactivated manually** After accessing the Outputs ON/OFF section (User Menu) the user can activate/deactivate the duly programmed outputs.
- The **Menu Sections** are the authorized User menu sections (refer to paragraph *2-5-1 Accessing the User Menu, point 1.*)
- **Customized Shortcuts**. Each code can be programmed to manage:
  - •• up to 12 customized (personal) shortcuts assigned to keys F1 Fn, ..., F4
  - •• up to 10 customized (personal) shortcuts assigned to keys 0 ␣, ..., 9 wxyz
  These shortcuts are available only after accessing the User Menu.



Accessing the User Menu 2-5-1

In order to access a customized (personal) menu, it is necessary to type the respective PIN and press key OK.

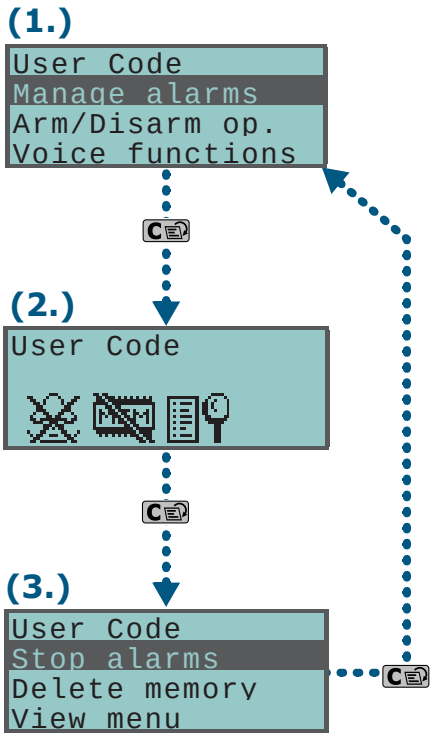
At this point, there are 3 different ways of allowing first-access to the user menu, depending on the system setup, as follows.

1. The user can access the menu directly, as shown in the figure opposite *(1.)*; using keys and , the user can select the desired menu section and press OK for access. Following is a the list of available User-Menu sections:

- Manage alarms
- Arm/Disarm op.
- Voice functions
- Activations
- View
- Outputs ON/OFF
- Set date/time
- Set Keypad
- Change PIN
- TelephoneNumbers
- Teleservice req.
- Overtime
- Thermostat

2. The keypad cancels the shortcut icons associated with keys F1 Fn, ..., F4 and replaces them with the customized shortcut icons associated with the code, as illustrated opposite *(2.)*; using keys F1 Fn, ..., F4 and 0 ␣, ..., 9 wxyz select the desired shortcut.
3. You can access a descriptive menu of the customized shortcuts assigned to keys F1 Fn, ..., F4 as opposite *(3.)*. To activate the shortcuts use key or to scroll for the description of the required shortcut then press OK.

All methods allow first access to the menu after a valid code-entry followed by OK. At this point, each time you press key C, 3 different objects will appear, select the one that applies to the operation concerned and then continue.



Keys 2-6

The SmartLiving system is capable of managing INIM's contact-free digital-keys, which are available in three versions:

- **nKey** - proximity keyfob
- **nCard** - proximity card
- **Air2-KF100** - wireless keyfob

Each key is unique and is identified by a random code selected from over 4 billion code combinations. During the installation phase, each key is enrolled on the system in order to allow it to operate.

Each key is characterized by the following parameters (programmed by the installer) in accordance with the requirements of the key user.

- **Partitions** - User codes can control only the partitions they are assigned to. If a key is used at a reader, it can operate only on the partitions the two devices have in common. For example, if the key controls partitions 1, 3, and 5 and the reader controls partitions 1, 2 and 6, the key can operate on partition 1 only, as it is the only partition the key and reader have in common. If a keyfob button is pressed, the user will be allowed access only to the partitions the wireless keyfob is assigned to.
- Up to 4 **Shortcuts**.
- A **Timer** can be set up to restrict the use of a key. The system will allow the key to operate the system only when the Timer is active. In this way, the user will be unable to access the system at all other times.
- **Patrol** attribute - This option is usually enabled on keys used by security personnel or night watchmen who must patrol the protected premises at regular intervals. This type of key does not allow the user to select the "Arm Type". When a key with this attribute is recognized, the system will perform the following operations:

1. Disarm the partitions common to the key and reader concerned.
2. Activate the respective Patrol Time for the partitions concerned.
3. Re-arm the partitions (as before) when the Patrol Time expires.

If the patrol key is held in the vicinity of the reader while the Patrol Time is still running (for example, if the inspection ends ahead of time), the Patrol Time will end immediately and the partitions will arm as before.

- **Maintenance** option - On acceptance of a key with this attribute, the system will deactivate any outputs associated with Zone alarm/tamper and Partition alarm/tamper events (on the Partitions the key and reader have in common). This type of key can select the reader shortcuts and its customized (personal) shortcuts.

Air2-KF100 Wireless keyfobs 2-6-1

The KF100 keyfob has 4 remote-control buttons which can each be programmed with a shortcut (ask your installer for details). The graphic-choice feature allows you to identify the buttons by numbers or icons.

The keyfob also provides 4 button-associated LEDs and a confirmation LED. As a result of two-way communications with the BS100 transceiver, the KF100 keyfob imparts audible and visual feedback signals (beep and LED signals) which notify the user of the outcome of requested operations.

Technical specifications	Value
Battery	3V CR2032 Lithium battery (included)
Buzzer	Multitone
Rubber pushbutton version	- with icons - with numbers

Table 9: **Feedback signals provided by KF100**

Push button	Icon	LED 1	LED 2	LED 3	LED 4	Buzzer signal	Operation
F1		1 flash				beep	Shortcut activation 1
F2			1 flash			beep	Shortcut activation 2
F3				1 flash		beep	Shortcut activation 3
F4					1 flash	beep	Shortcut activation 4
F2 + F3	+		1 flash	1 flash		beep	Block/Unblock keyfob
any				4 flashes	4 flashes		Keyfob blocked

Note

If an operation is successful, but the corresponding LED fails to light, it is an indication that the battery is low.
The battery must be replaced before it runs out completely.

Feedback from panel	Confirmation LED - green	Confirmation LED - red	Buzzer signal
Command not received		1 flash	
Operation not done		4 flashes	bop (audible error signal)
Operation done	3 flashes		long beep

Multi-system access 2-7

Users can access several systems using the same code/key/keyfob. The user code, key or keyfob must be enrolled separately on the control panels concerned, and can be programmed with different attributes and functions in accordance with the requirements of each specific system.

The keys and codes provide the systems with random codes (for keys) or PINs (for codes) which the system associates with the respective attributes and functions programmed by the installer. For example, a user key/code may be enabled on partitions 1 and 2 on system A, on partitions 7, 8 and 9 on system B and on partitions 4 and 5 on system C.

This operating method is possible for all keys and codes.

Telephone functions 2-8

The SmartLiving control panel events can be programmed to trigger report calls to an Alarm receiving Centre (via digital dialer) and also voice calls and SMS messages to contact numbers.

The SmartLiving control panel also accepts commands over-the-phone. Shortcut commands can be sent during calls to/from the control panel, after valid PIN entry on the telephone keypad.

The commands can be activated by keys "**0**" to "**9**" on the telephone keypad, which the system associates with various shortcut actions. Each code can be programmed with customized shortcuts, such as: arm, disarm, activate/ deactivate outputs, delete alarm memory, etc.

If the system is equipped with a SmartLogos30M voice board, the code shortcuts assigned to keys "**0**" to "**9**" will be announced over-the-phone, in order to facilitate operations.

Additionally, the Listen-in function allows you to eavesdrop on the protected premises by means of the keypad microphones.

When a user requests an operation - via a correctly formatted SMS message or voice call to the SIM card of the Nexus - the control panel will activate the respective shortcut/event and send confirmation (feedback) of the successfully implemented command.

WEB / e-mail functions 2-9

All SmartLAN/G equipped SmartLiving control panels are capable of sending event associated e-mails (SmartLAN/G is an optional accessory board).

The e-mail text, subject, attachments and recipients must be edited by your installer. No changes whatsoever should be made to the e-mail structure. Each e-mail text is capable of containing a direct link to a website or to an IP addressable device such as an IP camera, and an attachment document/file.

For a description of a typical e-mail format, refer to paragraph *5-17-1 e-mail*.

In addition to e-mails, the SmartLAN/G board allows you to interface with the control panel from any computer or mobile phone device (PDA, mobile phone, etc.) via any internet browser. The SmartLAN/G board integrates a web-server which allows users to operate the control panel from remote locations without the need of authentication.

For further details regarding the web-server, refer to paragraph *5-17-2 Access the web-server*.

Arming scenarios 2-10

A scenario is a pre-set arming configuration which applies various operating modes to the SmartLiving system partitions (the scenarios are programmed by the installer in accordance with user requirements).

For example, if all the occupants are leaving the building, you can apply a scenario that arms all the partitions and activates the outputs which closes the rollerblinds and switches off the lights. On returning to the building, you can apply a scenario that disarms some of the partitions (those required) and activates an output which switches on the garden lights.

The installer will set up the and make available the scenarios which best suit user requirements. The scenarios can be activated via keypad, reader, remote-control, and over-the-phone using shortcut commands (refer to *Chapter 3 - Shortcuts*), or through a web-server with a mobile-phone interface, by accessing the "Scenario activation" section (paragraph *5-17-3 Mobile-phone web interface*).

Chapter 3

SHORTCUTS

Keypad shortcuts

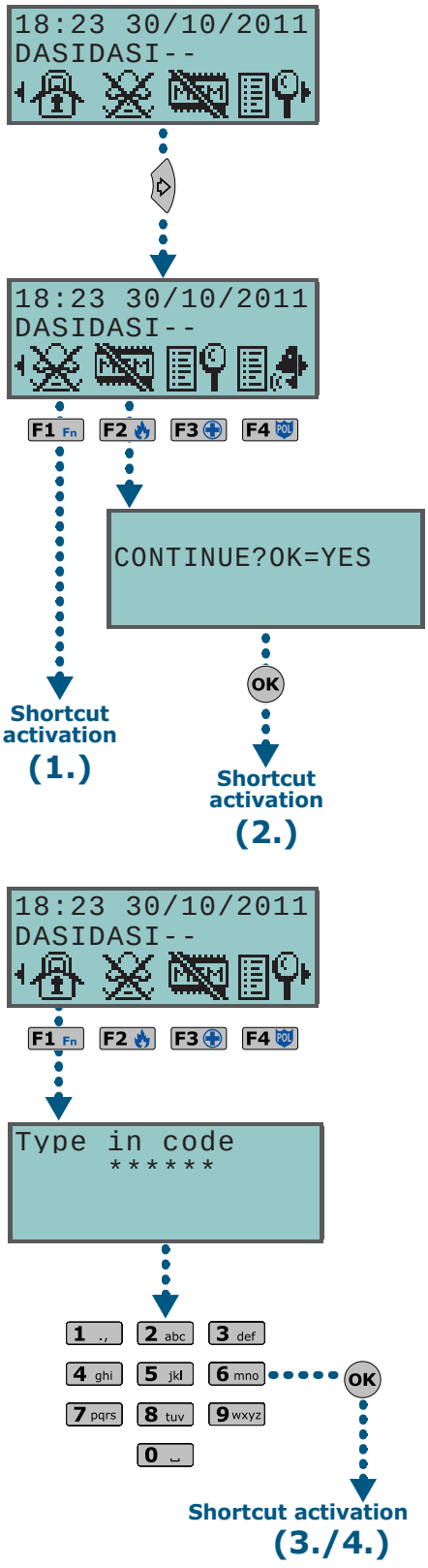
Each keypad can be programmed with up to 12 shortcuts associated with 4 function keys F1 F2 F3 F4. The shortcuts are identified by icons which appear on the lower part of the display. Arrows to the right and left of the icons indicate that keys ◁ and ▷ will allow you to view and use other shortcuts (if programmed).

The 12 keypad shortcuts can be activated in 4 different ways, as follows.

1. **By ALL**. Press the respective key F1, ..., F4 to activate the shortcut instantly without code entry. The shortcut will affect all the keypad partitions.
2. **By ALL with confirmation request**. Press the respective key F1, ..., F4, the system will ask if you wish to continue or not. If you press OK the shortcut will activate instantly, if you press C or Esc the operation will be abandoned. This method protects against accidental operations. The shortcut will affect all the keypad partitions.
3. **Code users only**. Press the respective key F1, ..., F4 then enter a valid code, the shortcut will activate after code recognition. The shortcut will affect the partitions common to both the keypad and code.
4. **Code users only when activation of the shortcut lowers system security**. If a shortcut involves a scenario that completely disarms a partition, or switches a partition from Away mode to Stay mode, the security of your system will obviously be at risk, therefore, the system will request code entry. The shortcut will affect the partitions common to both the keypad and code.

To activate a shortcut, press the key F1, ..., F4 which corresponds to the shortcut icon. The system will either activate the shortcut instantly (case 1.) or will request confirmation (case 2.) or code entry (cases 3. and 4.) before carrying out the operation.

3-1



Shortcut with code 3-2

Besides the keypad shortcuts provided by keys F1 Fn F2 F3 F4, each user code can have as many as 22 customized (personal) shortcuts.

Users can access their code-shortcuts only after entering their PINs and pressing OK (refer to paragraph *2-5-1 Accessing the User Menu*). Each code can be programmed to manage:

- Up to 12 shortcuts activated by keys F1 Fn, ..., F4 and identified by explicit icons.
- Up to 10 shortcuts activated by keys 0 ␣, ..., 9 wxyz. If a code is enabled to operate the system over-the-phone, these shortcuts will also be available on the telephone number-keys.

Entry of a code associated with shortcut no.9: at a JOY/MAX keypad, prompts the voice announcement of all the shortcuts assigned to the number keys.

To activate a shortcut at a keypad, work though the following steps.

1. Type in your code then press OK.
2. Access the User Menu, using the method described in paragraph *2-5-1 Accessing the User Menu* at point 2.
3. Press the key F1 Fn, ..., F4 which corresponds to the shortcut icon or press the key 0 ␣, ..., 9 wxyz which is assigned directly to the shortcut.

To activate a shortcut over-the-phone:

1. Establish communication with the control panel.
2. Type in your code followed by "**#**".
3. Listen to the voice prompts regarding the available shortcuts.
4. Press the number key which corresponds to the required shortcut.

Key and Reader shortcuts 3-3

nBy/S and nBy/X Reader shortcuts 3-3-1

Hold a valid key in the vicinity of the reader, as soon as the reader accepts the key, a series of visual signals on the reader LEDs will indicate the various shortcuts.

When the required shortcut is indicated, remove the key to activate the corresponding shortcut action.

The visual signals on the Reader LEDs are as follows (refer to *Table 7: Reader LEDs with key at reader*).

1. **Red LED on for 3 seconds** - shortcut associated with the red LED of the reader or first shortcut of the key
2. **Blue LED on for 3 seconds** - shortcut associated with the blue LED of the reader or second shortcut of the key
3. **Green LED on for 3 seconds** - shortcut associated with the green LED of the reader or third shortcut of the key
4. **Yellow LED on for 3 seconds** - shortcut associated with the yellow LED of the reader or fourth shortcut of the key
5. **All LEDs on for 3 seconds -** first shortcut associated with the user key
6. **All LEDs off for 3 seconds** - disarm all the partitions.
7. If the key is not removed, the reader will run through the entire sequence again starting from the red LED. Selection of the desired shortcut (indicated by a specific LED) will not occur until the key is removed.

If, during this phase, any of the partitions are armed, the LED sequence will start at point 6.

If the installer has enabled option "50131ReadLedOFF", the reader LEDs will be off, therefore, if you wish to activate a shortcut, you must:

1. Wave the key across the sensitive area of the reader: the LEDs will signal the respective status for 30 seconds.
2. During this 30 second period, hold a valid key in the vicinity of the reader in order to generate the visual signals on the reader LEDs. Remove the key when the required operation or pre-set scenario is indicated on the LEDs.

Shortcuts on JOY/MAX-keypad readers 3-3-2

Hold a valid key in the vicinity of the reader area of the JOY/MAX keypad, indicated by .

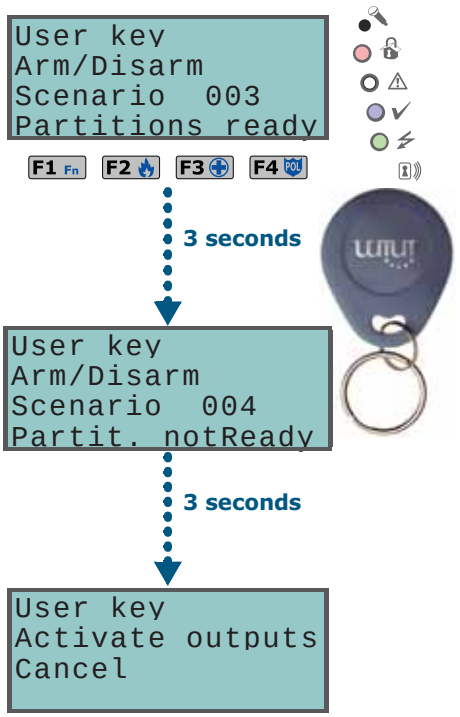
The key and reader shortcuts will flash one-by-one at 3 second intervals on the keypad display.

When the required shortcut is indicated, remove the key to activate the corresponding action.

The shortcuts appear on the display in the following order:

1. **Description of the first reader shortcut for 3 seconds**
2. Description of the second reader shortcut for 3 seconds
3. Description of the third reader shortcut for 3 seconds
4. **Description of the fourth reader shortcut for 3 seconds**
5. **Description of the fourth reader shortcut for 3 seconds**
6. **"Disarm"** (disarms all the partitions) for 3 seconds
7. Then back to point 1. if the key is not removed.

If, during this phase, any of the partitions are armed, the LED sequence will start at point 6.



Keyfob shortcuts 3-3-3

To activate the shortcuts (programmed by your installer) assigned to the 4 keys **F1**, ..., **F4** on the keyfob, simply push the button which corresponds to the desired command. The successful outcome of the operation will be signaled by the buzzer and feedback LEDs on the keyfob (refer to *Table 9: Feedback signals provided by KF100*).

Shortcut list 3-4

For the complete list of shortcuts refer to the table in *Appendix B, Shortcuts at default*.

Shortcuts 0 to 8, shown in the table, carry out the specified actions instantly.

Shortcut 9 can be activated over-the-phone only (telephone shortcut).

Shortcut 17 can be activated over-the-phone or at a keypad.

All other shortcuts (from 10 to 16 and from 18 to 37) provide direct access to specified sections in the User Menu, therefore, can be activated at keypads only.

Chapter 4

VOICE FUNCTIONS

If the SmartLiving control panel is equipped with a SmartLogos30M voice board, you will be able to take advantage of all the voice functions provided by the JOY/MAX keypad, and the over-the-phone voice guide.

Your installer will program the voice messages you require:

- for event-associated calls
- for event-associated announcements on the JOY/MAX keypad at address 1

Each JOY/MAX keypad has a memo-box for user-memo recording/playback. This handy function will allow you to leave messages for other users who have access to the keypad; refer to paragraph *5-3 Voice functions and Intercom (JOY/MAX only)*. You can record, play and delete messages at your own discretion.

The presence of a new memo in the memo-box will be indicated on the blue LED on the keypad, as described in *Table 5: Keypad LEDs*.

The SmartLogos30M voice board provides a total of 60 seconds memo time (shared by all the JOY/MAX keypads in the system).

Note

15 memo slots are available.

Chapter 5

USING THE SYSTEM

This chapter describes all the operations users can carry out with or without authorization (user PIN entry). The tools and methods which allow access the system operations are as follows.

The system can be accessed:

- Via **keypad** (JOY/GR, JOY/MAX, nCode/G, Concept/G).
  The keypad allows users to operate the system:
  1. By means of shortcuts (refer to paragraph *3-1 Keypad shortcuts*)
  2. By means of access codes via the User Menu (refer to paragraph *2-5 User Codes* and paragraph *3-2 Shortcut with code*) Users have various ways of viewing their personal menus (refer to paragraph *2-5-1 Accessing the User Menu*), however, this chapter describes the procedure via menu and provides the visual information relating to the sections described at point 1 in paragraph *2-5-1 Accessing the User Menu*.
- Via **Reader** (nBy/X, nBy/S, built-into JOY/MAX keypads)
  This proximity-key reader provides users with only one way of accessing the system, as described in paragraph *3-3 Key and Reader shortcuts*.
- **Over-the-phone**
  During a call from/to the control panel after valid code (PIN) entry.
- Via **Command Zone**
  After violation of a duly-programmed zone which sends a command to the control panel.
- Via **Wireless keyfob**
  by means of keys **F1**, ..., **F4** as described in paragraph *2-6-1 Air2-KF100 Wireless keyfobs*.
- Via **Web**
  by means of the integrated web-server on the SmartLAN/G (if installed) via any browser (refer to paragraph *5-17-2 Access the web-server*).

Managing alarms 5-1

This paragraph describes the actions users can take during typical alarm and tamper conditions:

- **Stop alarms** - deactivates instantly the outputs activated by zone/partition alarm and tamper events and system tamper events.
  The system tamper events are:
  - •• Open panel
  - •• Dislodged panel
  - •• Peripheral tamper (expansion, keypad, reader)
  - •• Peripheral loss (expansion, keypad, reader)
- **Clear call queue** - clears the outgoing call queue and stops any ongoing calls.
- **DeleteAlarm mem.** - implements a "Stop alarms" operation and, at the same time, deletes memory of system and partition alarm and tamper events.

Via Keypad

Method 1

Activate the shortcuts associated with keys F1 Fn, ..., F4 (shown on the display) with or without code entry.

- The shortcut which is assigned to "Alarm menu" operations (shortcut n.13:) allows you to view the respective section. You can select one of the following options, using and activate it by means of the OK key:
  - **Stop alarms**
  - **Clear call queue**
  - **DeleteAlarm mem.**
- The following shortcuts activate the associated commands:
  - Shortcut n.2: "Stop alarms"
  - Shortcut n.3: "Clear call queue"
  - Shortcut n.4: "DeleteAlarm mem.";

Method 2

Access the "Alarm management" section (User Menu) by means of a valid PIN.
Follow the instructions described in **Method 1**.

Via Reader

Hold a valid key in the vicinity of the reader until the reader LEDs or display indicates "Stop alarms" (shortcut n.2), "Clear call queue" (shortcut n.3) or "DeleteAlarm mem." (shortcut n.4).

Over-the-phone

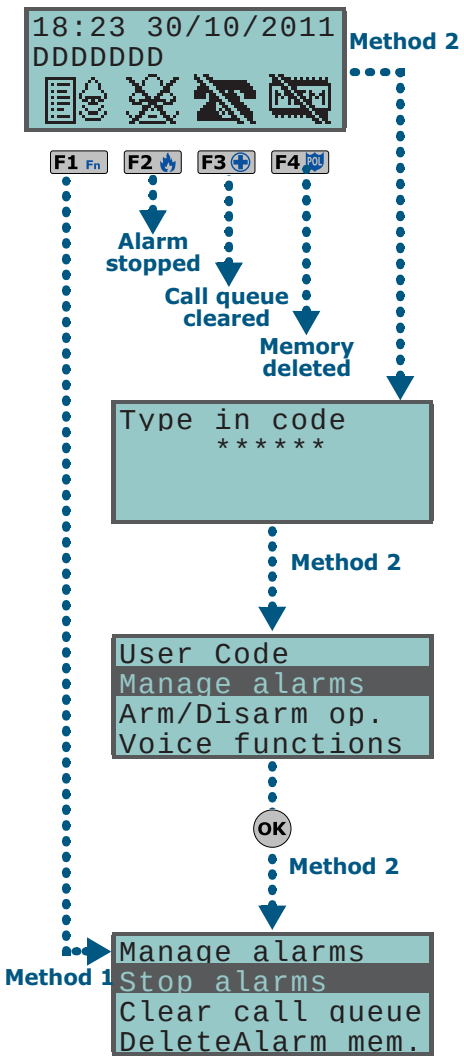
Type-in the PIN of a user code followed by "**#**" (the user code must be enabled to operate the system over-the-phone), then press the key (from "**0**" to "**9**") which the installer has programmed to activate "Stop alarms" (Shortcut n.2), "Clear call queue" (shortcut n.3) or "DeleteAlarm mem." (shortcut n.4).

Via Wireless keyfob

Push the respective button on the keyfob and verify the outcome of the requested operation, as described in paragraph *2-6-1 Air2-KF100 Wireless keyfobs*.

Via Web

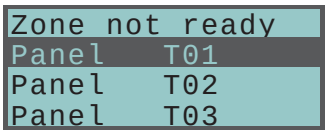
Access the SmartLAN/G web-server and press button. Use the mouse to select a partition then press button to delete the alarm memory and, if allowed, tamper memory.



Arming and disarming partitions 5-2

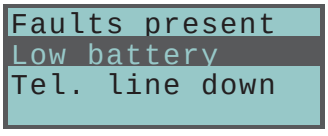
You can arm/disarm the system partitions via keypad, reader, over-the-phone, zone command, wireless command, Internet, as follows.

If you enter an arm-partition/s command at a keypad and not all the respective zones are in standby status (thus execution of the command would generate an instant alarm), the keypad will provide a list of the zones concerned, as shown in the figure opposite.



Use keys and to scroll the list and view the zones which are not in standby status. If you wish to go ahead with the operation despite the consequences, press OK. In this case, you will trigger an instant alarm on the zones indicated on the display.

If you enter an arm-partition/s command at a keypad and conditions (programmed by the installer) which lower the security of the system are present, the keypad will provide a list of the conditions concerned, as shown in the figure opposite.



Use keys and to scroll the list and view the conditions which lower the security of the system.

If you wish to go ahead with the operation despite the consequences, press OK. Arming the system under such circumstances will generate a "Forced arming" on partition event. This event highlights the fact that partitions were armed when conditions which lowered the security of the system were present (for example, "Low battery" or "Mains failure"). If, however, the installer included the "LossTamp.ongoing" event in the list of conditions which lower security, and this condition is active, you can cancel the operation by pressing OK.

Via Keypad

Method 1

Activate the shortcuts associated with keys F1 Fn, ..., F4 (shown on the display) with or without code entry.

- The shortcut which is assigned to "Arm/Disarm" operations (shortcut n.1:) applies the pre-set scenario.
- The shortcut assigned to "Arm/Disarm Menu" (shortcut n.12:), allows you to view the respective section and arm (in Stay or Away mode) or disarm each partition separately.

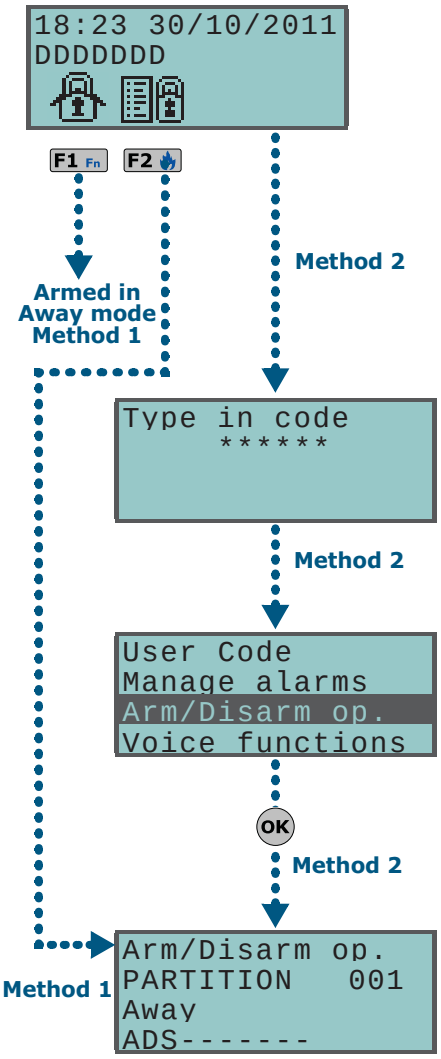
1. Select the desired partition, using keys and .
2. Select the required operating mode, using keys and .
3. Once the required operation has been selected, press .

Method 2

Access the "Arm/Disarm" section of the User menu by means of a valid PIN. Follow the instructions described in **Method 1**.

Method 3

While the entry time is still running (refer to "Entry Time" in *Appendix A, Technical terminology and Glossary*), type in a valid code followed by OK (the code must have access to the "Arm/Disarm" section of the User Menu), the partitions the code and keypad concerned have in common will disarm instantly.



Via Reader

Hold a valid key in the vicinity of the reader and remove it when "Arm/Disarm" (shortcut n.1) is indicated on the LEDs (the system will apply the pre-set scenario).

Over-the-phone

Type in a valid code PIN followed by "**#**". Press the number key (from "**0**" to "**9**") associated with the "Arm/Disarm" shortcut (shortcut n.1) in order to apply the pre-set scenario.

Via Command Zone

Under normal circumstances, a command zone comprises a mechanical key-lock or callpoint which activates an electrical contact wired to the command zone. In accordance with how the command zone is configured, it is possible to:

- arm the partitions the zone belongs to
- disarm the partitions the zone belongs to
- switch the status of the partitions (arm any disarmed partitions and disarm any armed partitions, refer to "Switch Zone" in *Appendix A, Technical terminology and Glossary*)
- arm the partitions the zone belongs to when the command zone is violated, and disarm the partitions the zone belongs to when it restores to standby

Via Wireless keyfob

Push the respective button on the keyfob and verify the outcome of the requested operation, as described in paragraph *2-6-1 Air2-KF100 Wireless keyfobs*.

Via Auto-arm operations

If a partition is associated with a timer which controls automatic-arming operations, it will arm when the timer switches ON and disarm when the timer switches OFF. Users who are enabled to control Auto-arm operations (refer to paragraph *5-4 Activations*) must:

- activate the timer associated with the Auto-arm operations
- enable the Auto-arm option for the partitions concerned

Via Web

Access the SmartLAN/G web-server and press button. Use the mouse to select a partition then press the buttons shown opposite to activate the operations.

Access the "Scenario activation" section, through the mobile-phone interface, press . Select the desired scenario from those available, by clicking-on the scenario label or icon . In response, the system shows the icons opposite:

Icon	Key
	Arm selected partition in Away mode
	Arm selected partition in Stay mode
	Arm selected partition in Instant mode
	Disarm selected partition

Icon	
	Scenario activated correctly
	Scenario not activated

Voice functions and Intercom
(JOY/MAX only)

5-3

Voice communication (during keypad-to-keypad intercom calls) is one-way, therefore, only one person should speak while the other listens. The user who wishes to speak must press OK on the keypad in use.

The voice functions are:

- **Record** - starts the recording phase of the memo in the memo-box of the keypad you are working on.
- **Playback** - starts the playback phase of the memo in the memo-box of the keypad you are working on.
- **Delete** - deletes the memo in the memo-box of the keypad you are working on.
- **Intercom** - allows two-way voice communication with another JOY/MAX keypad.

Via Keypad

Method 1

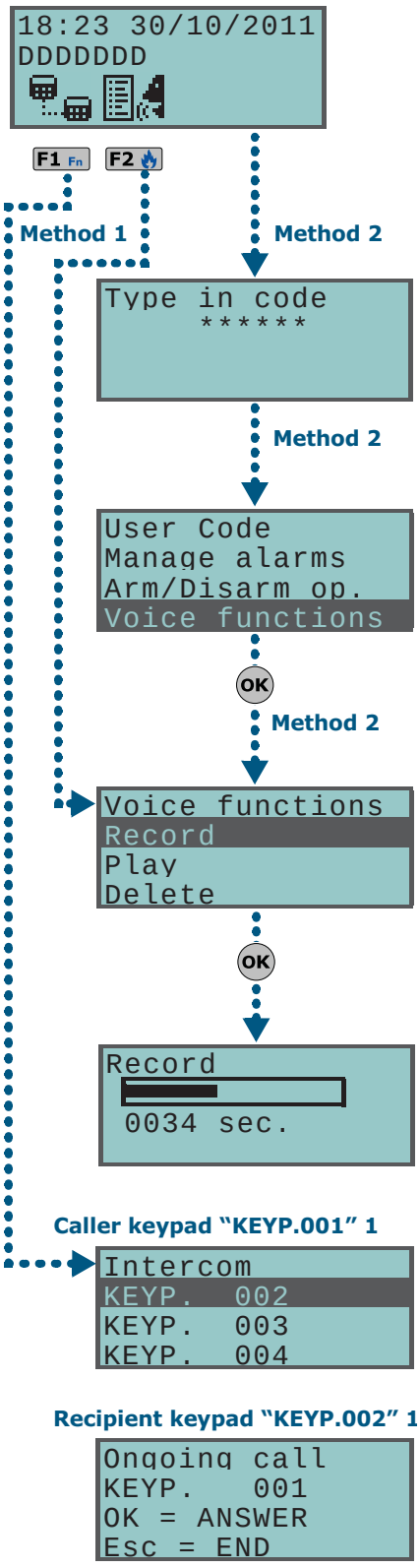
Activate the shortcuts associated with keys F1 Fn, ..., F4 (shown on the display) with or without code entry.

- The shortcut assigned to the "Voice functions menu" (shortcut n.14:) allows you to view the "Voice functions" section. Select the required function by means of keys e then press OK.
  - **Record/Playback** - the operation time-out (expressed in seconds) will be signaled by a counter and a progress bar on the display. If you wish to interrupt the record/playback operation manually, press OK, otherwise, it will end automatically when the pre-set time-out expires. You can adjust the volume during the playback phase using keys and .
  - **Delete** - this operation must be confirmed by pressing OK.
  - **IntercomCall -** the display provides the list of keypads you can call. Use and to select the keypad you wish to contact, then press OK to send the call. The recipient keypad will emit a series of beeps to signal an incoming call and the display will be as shown in the figure. The recipient can press OK to answer the call or Esc to reject it. Both the sender and the recipient can end the call by pressing Esc. The volume can be adjusted during the listen phase by pressing keys **and** .
- The "IntercomCall" shortcut (shortcut n.11:) allows you to view the previously described "Intercom call" section.

Method 2

Access the "Voice functions" section of the User Menu by means of a valid PIN.

Follow the instructions described in **Method 1**.



Activations

5-4

The activation/deactivation of the SmartLiving system peripherals and elements (described in the following section) enables them to operate in accordance with their settings (activation) or disables their functions completely (deactivation). The user has full control over activation/deactivation of the SmartLiving system peripherals and elements.

The following section describes the consequences of activation/deactivation.

- **Zone** - disabled zones cannot generate alarms (inhibited).
- **Auto-arm operations** - can be activated/deactivated separately on each single partition. If this option is enabled on a partition, it will arm and disarm in accordance with the On/Off settings of the respective timer.

- **Codes** - deactivated (disabled) codes cannot access the system.
- **Keys** - deactivated (disabled) keys cannot access the system.
- **Keypads** - deactivated (disabled) keypads cannot provide access to the system, therefore, cannot generate commands or shortcuts. However, the LEDs and display will be refreshed.
- **Readers** - deactivated (disabled) readers cannot provide access to the system, therefore, cannot accept keys or generate commands. However, the LEDs will indicate the current status of the system.
- **Timers** - activated timers (On) manage their associated elements (partitions, codes, keys) in accordance with their settings. Deactivated timers cannot time-manage their associated elements (partitions, codes, keys), therefore, they will function in accordance with Timer Off status.

Note

All the timers will be activated automatically when you exit the programming session. You must deactivate timers which are not used for system control purposes.

- **Dialer** - a deactivated (disabled) dialer cannot send voice or digital calls. However, if duly programmed, it will be able to manage incoming calls.
- **Answerphone function** - if activated (enabled), the control panel will answer incoming calls with the pre-recorded voice message ("Answerphone message").
- **Teleservice** - if activated (enabled), the installer will be able to access the system via modem. The Teleservice call allows the installer to work on the control panel parameters. Teleservice operations involve a request from you and the installers acceptance, therefore, this option needs to be enabled only when required.

Note

If the "Answerphone" and "Teleservice" functions are both enabled, the control panel will give incoming-call priority to the Teleservice call. After picking up the call, the control panel will allow the installer-company modem 30 seconds to establish communication. If the modem fails to communicate within this period, the control panel will play the pre-recorded "Answerphone" voice message.

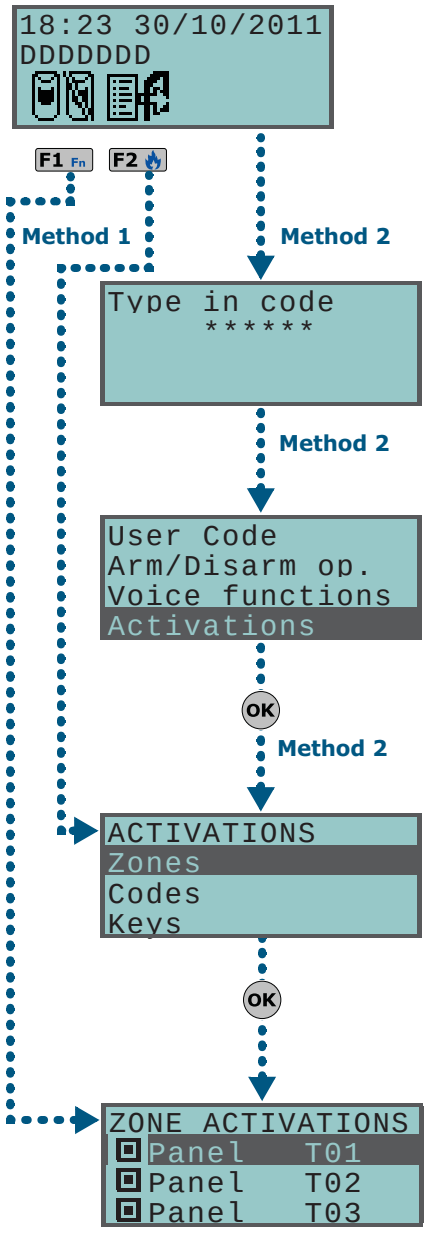
- **Internet access -** If this option is enabled, and the system is equipped with a SmartLAN/G board, the control panel will allow user-authorized access to the system via LAN/Internet. If this option is disabled, the control panel will allow user-authorized access to the system via Teleservice (if authorized).
- **Enable install.** If enabled, the Installer PIN will be accepted by the system and the installer will have access to the Installer menu. If disabled, entry of the installer PIN will generate an "Invalid Code" event and the installer will be denied access to the respective menu.

Via Keypad

Method 1

Activate the shortcuts associated with keys F1 Fn, ..., F4 (shown on the display) with or without code entry.

- The shortcut assigned to the "Activations menu" (shortcut n.15:), allows you to view the respective section in the User Menu.
  1. Use keys and followed by OK to select the category of elements you wish to activate/deactivate (zones, codes, etc.).
  2. Use keys and followed by OK, to select the single element you wish to activate/deactivate.
  3. Use * to activate the selected element or # to deactivate it.
- Other shortcuts which provide direct access to sub-sections of the "Activations" section are:
  - Shortcut n.19 ( ) accesses "Activations/Zones"
  - Shortcut n.22 ( ) accesses "Activations/Answerphone"
  - Shortcut n.23 ( ) accesses "Activations/Teleservice"
  - Shortcut n.24 ( ) accesses "Activations/Codes"
  - Shortcut n.25 ( ) accesses "Activations/Keys"
  - Shortcut n.26 ( ) accesses "Activations/Timers"
  - Shortcut n.27 ( ) accesses "Activations/Auto-arm"



Method 2

Access the "Activations" section of the User menu by means of a valid PIN.

Follow the instructions described in **Method 1**.

Via Web

Access the SmartLAN/G web-server (refer to paragraph *5-17-2 Access the web-server*).

Press the button. Use the mouse to select the partition and the zone (in the top section) then press the buttons shown opposite.

Icon	Key
	Deactivate (inhibited) the selected zone
	Activate (unbypass) the selected zone

View 5-5

This section allows you to view the events log and the current status of some of the system peripherals and elements.

The "Events log", "Alarms log", "Faults log" and "Arm/Disarm op." allow you to view the start and end of the corresponding events in chronological order.

The "Nexus status" section shows (on the display) some of the parameters of the Nexus dialer.

The "System voltage" section allows you to view the respective voltage panel.

The "Zone Status" section shows the status of the zone (Standby, Alarm, Shorted, Tamper) and Unbypassed/Inhibited status (Unbypassed - capable of generating alarms; Inhibited - incapable of generating alarms).

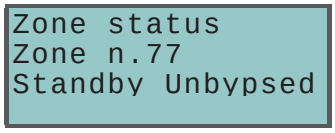
The "Faults" section allows you to view current faults only (refer to *Appendix C, Fault signals*).

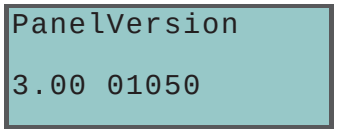
The "Panel version" section allows you to view the firmware version and model of your SmartLiving control panel.

When viewing the wireless zones, the last line on the display indicates the level of signal strength on a scale of 0 to 7; the higher the value the better the signal.

If you access the control panel via browser, it will be possible to view the status of:

- Partitions
- menu
- Outputs
- Timer
- Events log





Via Keypad

Method 1

Activate the shortcuts associated with keys F1 Fn, ..., F4 (shown on the display) with or without code entry.

- The shortcut assigned to "View menu" (shortcut n.16:), allows you to access the respective section in the User Menu and view the contents of the:
  - •• **Events log**
  - •• **Alarms log**
  - •• **Faults log**
  - •• **Arm/Disarm op.**

  User access to the information in the "Logs" is filtered. For example, a user can view only the zone alarms relating to the partitions the code and keypad concerned have in common. Press keys and to scroll the chronological events list.

  For some events, key allows you to view the partitions details. For example, the details of an "Arm" command will show the code and keypad concerned and, if you press , the list of partitions involved.

  - •• **Nexus status**:

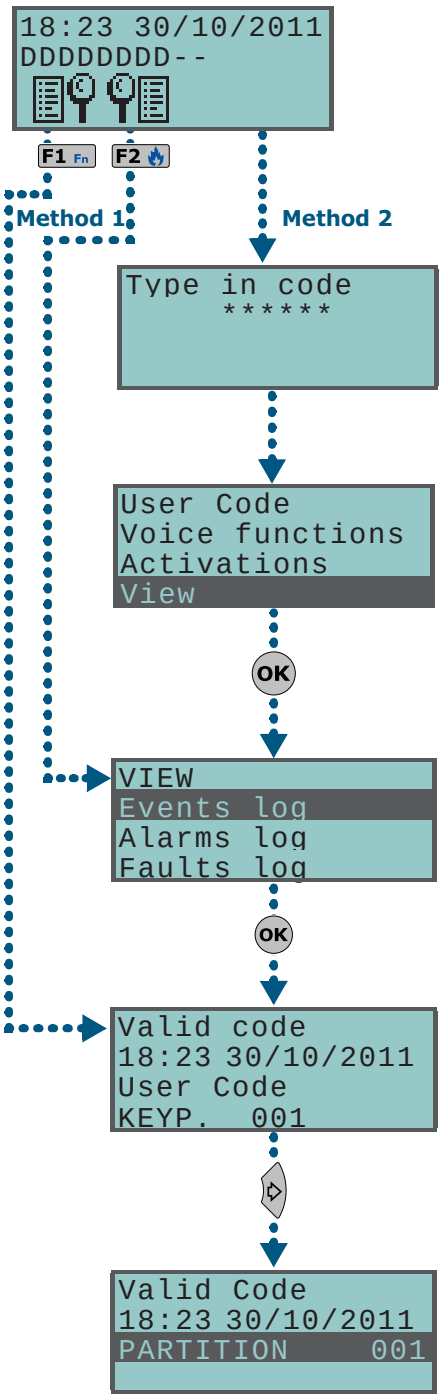
    The display will show the:

    1° line: GSM network provider (Vodafone, etc.)

    2° line: GSM signal reception (value between 1 and 100)

    3° line: balance, at the last operation (expressed in the local currency)

    4° line: faults; if present, access the "View-Faults ongoing" section for details



- •• **System voltage**
- •• **Zone status** - allows you to view only the zones associated with the partitions the code and keypad concerned have in common. Use keys and to scroll the list of accessible zones.
- •• **Faults**
- •• **PanelVersion**

• Other shortcuts which provide direct access to sub-sections of the "View" section are:

- •• Shortcut n.28 ( ) accesses "View/Events log"
- •• Shortcut n.29 ( ) accesses "View/Alarms log"
- •• Shortcut n.30 ( ) accesses "View/Faults log"
- •• Shortcut n.31 ( ) accesses "View/Arm/Disarm op."
- •• Shortcut n.32 ( ) accesses "View/System voltage"
- •• Shortcut n.33 ( ) accesses "View/Zone status"
- •• Shortcut n.36 ( ) accesses "View/Faults"

Method 2

Access the "View" section of the User menu by means of a valid PIN. Follow the instructions described in **Method 1**.

Via Web

Access the SmartLAN/G web-server (refer to paragraph *5-17-2 Access the web-server*).

Press the button. It is possible to view only the partitions the user controls:

Partition	Operating mode	Partition status		Alarm memory		Tamper memory		Auto-armed	
Description of the selected partition	Disarmed Away mode Stay mode Instant mode		Partition in standby status	empty	No alarm events saved to memory	empty	No tamper events saved to memory	empty	Disabled
			Partition in alarm status		Alarm event saved to memory		Tamper event saved to memory		Enabled
			Partition in tamper/short-circuit status						

Press the button. Use the mouse to select a partition and view (in the top section) all the partition zones the user controls:

Zone	Zone status		Inhibited status		Test		Alarm memory		Tamper memory	
Description of the zones which belong to the selected partition		Zone in standby status		Zone in inhibited status		Zone in test status	empty	No alarm events saved to memory	empty	No tamper events saved to memory
		Zone in alarm status		Zone unbypassed	empty	Zone not in test status		Alarm event saved to memory		Tamper event saved to memory
		Zone in tamper/ short-circuit status								

The outputs the user has access to will be shown in the field in the lower part of the zone section, after pressing the button if you are using a computer, or after pressing if you are using a mobile telephone device:

Output	Output status	
Output descriptions		Output activated
		Output deactivated

Press the button. It will be possible to view all the timers:

Timer	Timer status	
Timer description		Timer active
		Timer not active

Press the button then the Update Log button. It will be possible to view all the events saved to the log:

Number	Date/Time	Description	Partition involved	Source	Location	Category
Progressive number of the event	Date and time of the event (saved to the control panel-events log)	Event description	The group of partitions involved in the event (if applicable)	User ID or event trigger (if applicable)	Identification and location of the peripheral involved (if applicable)	Event category

Activating/Deactivating outputs 5-6

This section allows you to activate/deactivate manually the outputs the code controls.

Via Keypad

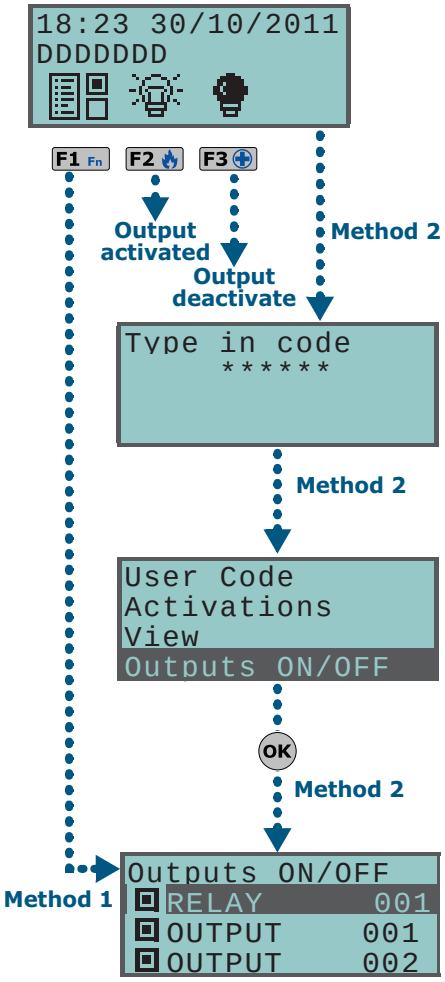
Method 1

Activate the shortcuts associated with keys F1 Fn, ..., F4 (shown on the display) with or without code entry.

- The shortcut assigned to "Output control" (shortcut n.21:), allows you to view the "Outputs ON/OFF"" section of the User Menu where you can:
  1. Use keys and to select the output you wish to activate /deactivate.
  2. Press * to activate the selected output or # to deactivate it.
- The shortcut assigned to the "Activate outputs" operation (shortcut n.5:) will activate the output when the respective button is pressed.
- The shortcut assigned to the "Deactiv. outputs" (shortcut n.6:) will deactivate the output when the respective button is pressed.

Method 2

Access the "Outputs ON/OFF" section of the User Menu by means of a valid PIN. Follow the instructions described in **Method 1**.



Via Reader

Hold a valid digital key in the vicinity of the reader until the reader LEDs or display indicates "Activate outputs" (shortcut n.5) or "Deactiv. outputs" (shortcut n.6).

Over-the-phone

Type-in the PIN of a user code followed by "**#**" then press the key (from "**0**" to "**9**") which the installer has programmed to trigger "Activate outputs" (shortcut n.5) or "Deactiv. outputs" (shortcut n.6).

Via Wireless keyfob

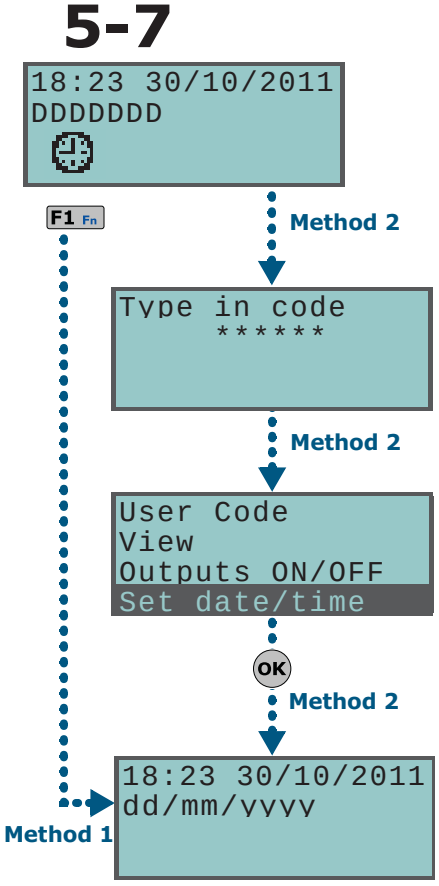
Push the respective button on the keyfob and verify the outcome of the requested operation, as described in paragraph *2-6-1 Air2-KF100 Wireless keyfobs*.

Via Web

Access the SmartLAN/G web-server (refer to paragraph *5-17-2 Access the web-server*) .The outputs the user has access to will be shown in the field in the lower part of the zone section, after pressing the button if you are using a computer, or after pressing if you are using a mobile telephone device. Select an output and activate or deactivate it using the buttons shown opposite:

Icon	Key
	Activate selected output
	Deactivate selected output

Change date and time



This option allows you to set the date and time in accordance with the selected format.

Via Keypad

Method 1

Activate the "Set date/time" shortcut (shortcut n.35:) associated with one of the following keys F1 Fn to F4 POL shown on the display, with or without code entry, to access the User Menu at the "Set date/time" section.

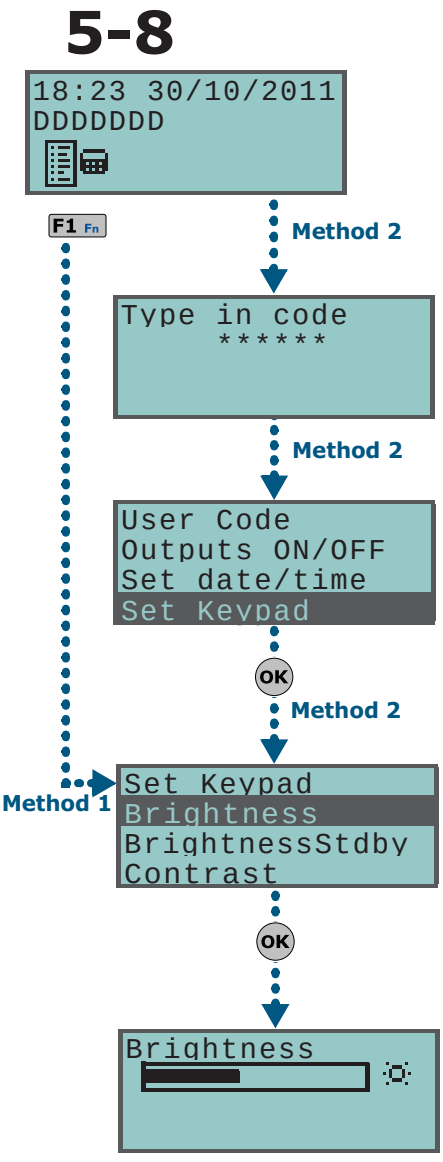
1. Use keys and to select the programming field (hour, minutes, etc.).
2. Use keys and to change the value in the selected field.
3. Press OK to save the setting.

Method 2

Access the "Keypad date/time" section by means of a valid PIN.

Follow the instructions described in **Method 1**.

Keypad settings



This option allows you to program the display and buzzer settings.

- **Brightness** - the level of brightness of the display backlight and LEDs when you press any key (duration 20 seconds).
- **Standby brightness** - the level of brightness of the display backlight and LEDs during standby status.
- **Contrast** - allows you to adjust the black/white contrast.
- **Volume** - allows you to adjust the buzzer volume (3 levels available).
  - Off
  - Low volume
  - High volume
- **Keypad options**:
  - **Temperature off** - if enabled, the temperature value (read by the built-in temperature sensor) will not be shown (JOY/MAX keypads only).
  - **NoExitTimeSignal** - if enabled, the buzzer will not emit audible signals during partition Exit time.
  - **NOEntryTimeSignal** - if enabled, the buzzer will not emit audible signals during partition Entry time.
  - **Beep on output** - if enabled, the buzzer will emit audible signals during partition Exit time.

These settings apply only to the keypad you are working on, and will be saved even in the event of panel shutdown.

Via Keypad

Method 1

Activate the shortcut assigned to the "Keypad set.menu" (shortcut n.18:), and associated with one of the following keys F1 Fn, ..., F4 POL (shown on the display), with or without code entry, to access the "Keypad settings"section of the User Menu.

1. Use keys and followed by OK to select the required parameters.
2. Use keys and to increase or decrease the value of the selected parameter. To activate the selected option press *, to deactivate it press #.
3. Press OK to save.

Method 2

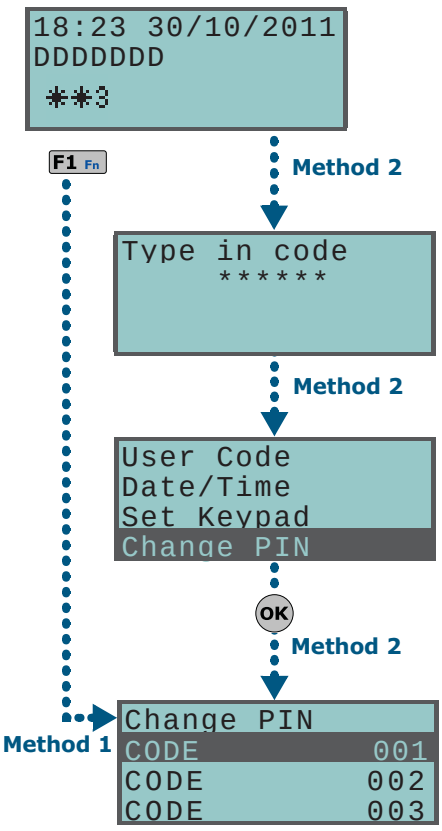
Access the "Keypad Settings" section of the User Menu by means of a valid PIN.

Follow the instructions described in **Method 1**.

Change PIN 5-9

This section allows you to change your User Code PIN. If your code has "Main User" status, it will also allow you to change the PINs of other users but not of other "Main Users".

In order to be EN50131 compliant, all PINs must have 6 figures.



Via Keypad

Method 1

Activate the shortcut assigned to the "Change PIN" (shortcut n.34: **3) and associated with one of the following keys F1 Fn, ..., F4 (shown on the display), with or without code entry, to access the "Change PIN" section of the User Menu.

1. Use keys and followed by OK the user code you wish to change.
2. Type-in the new PIN (4, 5 or 6 digits) using keys 0 ␣, ..., 9 wxyz then press OK.
3. Type-in the new PIN again using keys 0 ␣, ..., 9 wxyz then press OK to save.

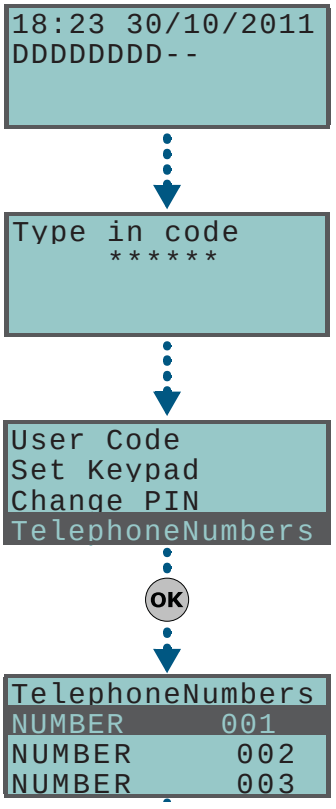
Method 2

Access the "Change PIN" section of the User Menu by means of a valid PIN.

Follow the instructions described in **Method 1**.

Change telephone numbers 5-10

This section allows users to change the contact telephone numbers. Only contact numbers with at least one partition in common with the entered PIN and keypad in use will be shown.



Via Keypad

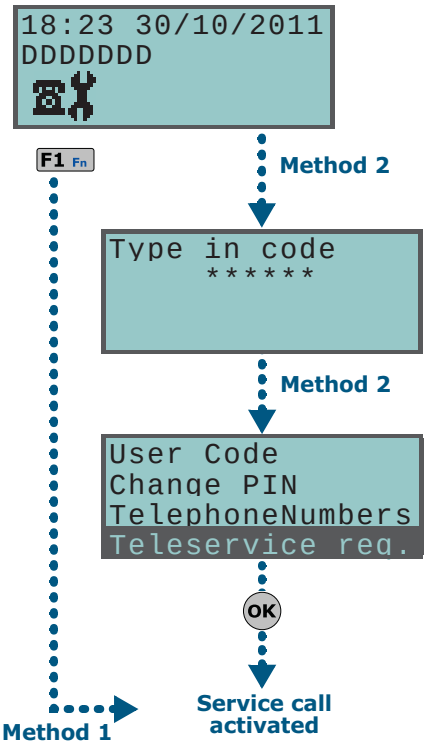
Access the phonebook:

1. Use keys and to select the required phone number then press OK; each programming field accepts a 20 digit phone number.
2. Use keys and to select the field you wish to change, then use the number keys (1 ., etc.) to edit the number. Accepts also "," (= 2 second pause), "*" and "#".
3. Press OK to confirm and exit.

Teleservice request 5-11

This command sends a call to the installer company.

Your installer must enable control panel option "Num10ForTeleserv", otherwise this function will not be available.



Via Keypad

Method 1

Activate the shortcut assigned to the "Teleservice req." (shortcut n.8: ☎).

Method 2

Access the "Teleservice" section of the User menu by means of a valid PIN.

Via Reader

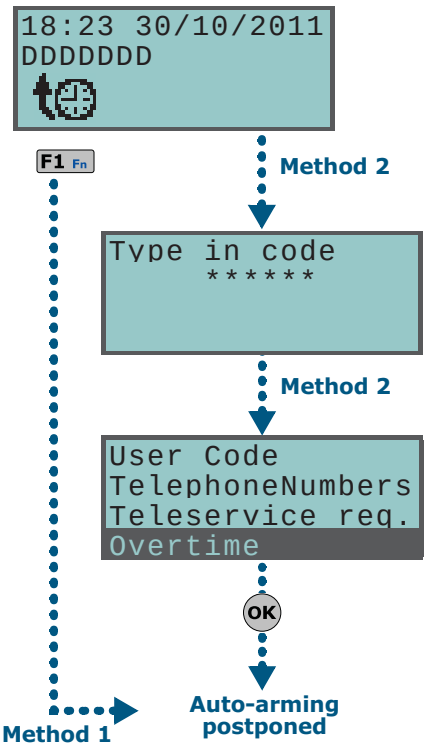
Hold a valid digital key in the vicinity of the reader until the reader LEDs or display indicates "Teleservice Request" (shortcut n.8).

Overtime request 5-12

This operation can be carried out under the following conditions only.

- The partition concerned must be timer-controlled.
- The auto-arm option must be enabled (refer paragraph *5-4 Activations*).

Each overtime request postpones the auto-arming operation by 30 minutes.



Via Keypad

Method 1

Activate the shortcut assigned to the "Overtime" (shortcut n.7:).

Method 2

Access the "Overtime req." section of the User Menu by means of a valid PIN.

Via Reader

Hold a valid digital key in the vicinity of the reader until the reader LEDs or display indicates "Overtime" (shortcut n.7).

Over-the-phone

Type-in the PIN of a user code followed by "**#**", then press the key (from "**0**" to "**9**") which the installer has programmed to activate "Overtime" (shortcut n.7).

Via Wireless keyfob

Push the respective button on the keyfob and verify the outcome of the requested operation, as described in paragraph *2-6-1 Air2-KF100 Wireless keyfobs*.

Thermostat 5-13
(JOY/MAX keypads only)

The "Thermostat" function, provided by JOY/MAX keypads, manages the heating or air-conditioning system in accordance with its setting.

- - **Summer**: when the sensor detects that the temperature has risen above the value set by the user, the output connected to the air-conditioning system will activate (indicated on the display by).
- - **Winter**: when the sensor detects that the temperature has fallen below the value set by the user, the output connected to the heating system will activate (indicated on the display by).

This function provides 5 operating modes for the user to choose from:

- **Off** - the thermostat is off; the output associated with the heating or air-conditioning system is deactivated.
- **Manual** - the temperature set by the user is valid for 24 hours per day, for 7 days per week.
- **Daily** - the temperature set by the user is valid during the selected hours for 7 days per week.
- **Weekly** - the temperature set by the user is valid during the selected hours on specific days of the week.
- **Antifreeze** - this is a forced operation. If the temperature drops below 2°C, the output connected to the heating system will activate.

Via Keypad

Method 1

Activate the shortcut assigned to the "Thermostat" (shortcut n.37:), and associated with one of the following keys F1 Fn, ..., F4 (shown on the display), with or without code entry, to access the "Thermostat" section of the User Menu."

1. Use the number keys to select the operating mode of the thermostat:
   - 1 .,- Thermostat Off
   - 2 abc - "Manual"
   - 3 def - "Daily"
   - 4 ghi - "Weekly"
   - 5 jkl - "Antifreeze"

   The display will show the:

   1° line: operating mode of the thermostat and day of the week

   2° line: pre-set temperature gauge and the "Summer/Winter" operating mode icon

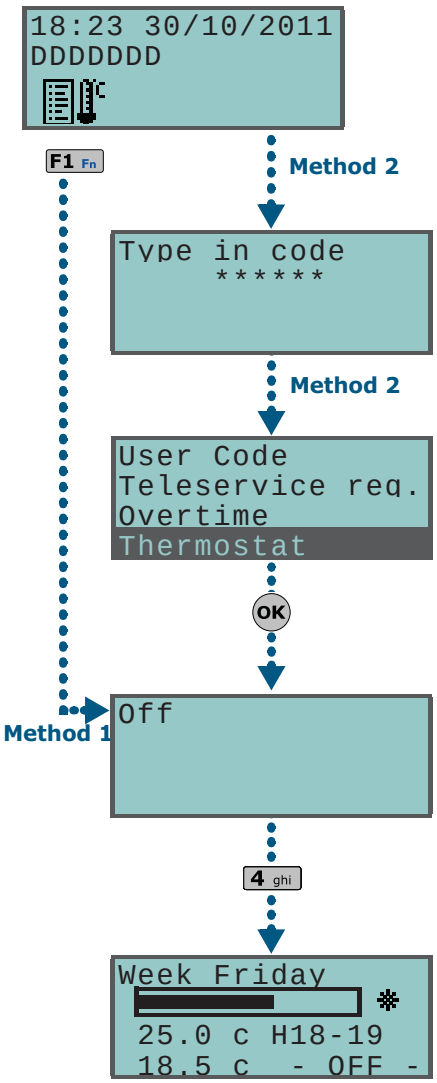
   3° line: temperature setting and operating hours

   4° line: temperature reading and the status of the heating system/air-conditioning system (ON/OFF)
2. Select the operating mode ("Summer/Winter") of the thermostat using 6 mno.
3. Select the temperature, using keys and .
4. Select the operating hours, using and .
5. Select the day of the week, using * and #.
6. Press OK to exit and save.

Method 2

Access the "Thermostat" section of the User Menu by means of a valid PIN.

Follow the instructions described in **Method 1**.



Listen-in 5-14

This function can be activated over-the-phone only.

The listen-in function allows you to eavesdrop on the protected premises through the microphones of JOY/MAX keypads which have at least one partition in common with the entered PIN.

Shortcut n.10 must be assigned (by your installer) to one of the number keys relating to the code that generates this operation.

Over-the-phone

Type-in the PIN of a user code followed by "**#**", then press the key (from "**0**" to "**9**") which the installer has programmed to activate "Listen-in" (shortcut n.10). The control panel will open a listen-in channel between the phone and the first JOY/MAX keypad configured in the system with at least one partition in common with the entered PIN. To open a voice-communication channel with another JOY/MAX keypad during the listen-in phase, press the number key which corresponds to the address of the keypad you wish to use. Also in this case, the selected keypad must have at least one partition in common with the entered code.

Press "*****", to end the listen-in phase and step back to the voice-announced Shortcut menu.

Partition status enquiry 5-15

This function can be activated over-the-phone only.

The Partition status enquiry function allows you to listen to voice announcements regarding of the armed/disarmed status of the partitions during telephone communications with the control panel, or by activating the corresponding shortcut from a JOYMAX keypad. The control panel will announce the armed/disarmed status of the partitions the entered PIN is assigned to.

Note

If you activate this shortcut from a JOY/MAX keypad, the control panel will announce the armed/disarmed status of the partitions the entered PIN is assigned to, regardless of the keypad partitions.

The user code must be enabled (by the installer) to activate shortcut n.17 via keys F1 Fn, ..., F4 VOL or the number keys.

Over-the-phone

Type-in the PIN of a user code followed by "**#**" then press the key (from "**0**" to "**9**") which the installer has programmed to activate "Arming status" (shortcut n.17). The control panel will announce (in order) the descriptions of the partitions the entered PIN is assigned to and their current armed/disarmed status.

Press "*****", to step back to the main menu to listen to all the voice announcements relating to the entered PIN.

Via Keypad

After entering a valid user-code PIN, press the key which is assigned to the "Arming status" shortcut (shortcut n.17). The control panel will announce (in order) the descriptions of the partitions the entered PIN is assigned to and their current armed/disarmed status.

Commands over-the-phone 5-16

Panel to user calls 5-16-1

Your installer will instruct you as to which events generate voice calls. Event report calls will be sent to the programmed contact numbers of your choice when the event occurs and, in most cases, also when it ends.

During the call, the call recipient can:

- press "*****" to go to the next message or, if there is only one message, end the successful call.
- Type-in a valid PIN followed by "**#**" and access the customized shortcuts assigned to the code. The control panel will activate the voice guide which will announce the available shortcuts and the number keys to press. The control panel will activate the corresponding shortcut as soon as the selected number is pressed on the telephone keypad.

User to panel calls 5-16-2

If the "Answerphone" function (refer to paragraph *5-4 Activations*) is enabled, users can call the control panel from any remote telephone and send commands to the system (refer to paragraph *3-2 Shortcut with code*) and/or activate Listen-in sessions (refer to paragraph *5-14 Listen-in*) in the following way.

1. Dial the control panel telephone number.
2. Allow the phone to ring for the pre-established number of rings. The control panel will answer and will play message n.216.
3. Type in your PIN followed by "**#**".
4. The control panel will activate the voice function which will announce the available shortcuts and the number keys to press.
5. As soon as the selected number is pressed on the telephone keypad, the control panel will activate the corresponding shortcut.

If the system is equipped with a Nexus dialer, the user can operate on the control panel via voice call to the SIM card of the Nexus. If duly configured (by the installer), the user will receive feedback (SMS text message or ring) from the Nexus relating to successfully implemented commands.

SMS text message to the user 5-16-3

If the system is equipped with a duly programmed Nexus dialer, the user may receive SMS text messages signaling that events have occurred.

If an event (which has been duly configured by the installer) occurs or restores, the control panel will send notification to the programmed users via SMS.

SMS text message to the control panel 5-16-4

If the system is equipped with a duly programmed Nexus dialer, the user can operate on the control panel by sending SMS text commands to SIM card of the Nexus.

Users who wish to activate a command via SMS text must enter the command details as follows:

<xxxxxx> <SMS Text>

where

- <xxxxxx> stands for the user's PIN
- a blank space must be keyed in after PIN entry
- <SMS Text> which is the command identifier - this parameter must be provided by your installer.

If duly configured (by the installer), the user will receive feedback (SMS text message or ring) from the Nexus relating to successfully implemented commands.

SMS TEXT AT DEFAULT

The SmartLiving control panel is programmed with five predefined default commands:

- Balance enquiry relating to the SIM card of the Nexus
  If the following SMS text message is sent:
  <xxxxxx> CREDIT BALANCE
  where <xxxxxx> stands for the user's PIN - the user will receive an SMS text message indicating the remaining credit (balance).
- Status enquiry relating to the Nexus
  If the following SMS text message is sent:
  <xxxxxx> STATUS
  where <xxxxxx> stands for the user-access PIN - the user will receive an SMS text message indicating the:
  - device name and firmware revision
  - GSM network provider
  - GSM signal reception level
  - device tamper status
  - BUS status
  - Balance (remaining credit)
- Inhibition (using the "EXC" or "ESC" command) or activation (using the "INC" command) of the control panel zones
  If the following SMS text message is sent:

<xxxxxx> EXC <zone description>

where:

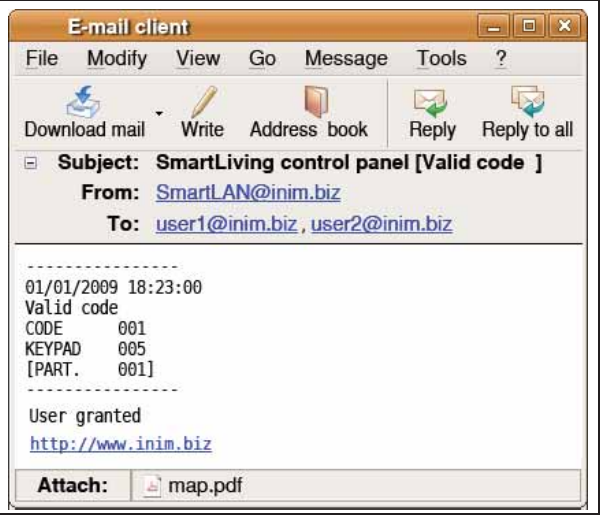
- <xxxxxx> is the PIN of a control-panel user coded, followed by a blank space
- "EXC" (or "ESC" or "INC") is the command to be implemented on the zone, followed by a space
- <zone description> is the name zone to be inhibited or activated

Using the SmartLAN/G 5-17

e-mail 5-17-1

The event-related e-mail sent to the user via the SmartLAN/G board must be programmed entirely by the installer.

Below is an example of an e-mail associated with a "Valid Code" event.

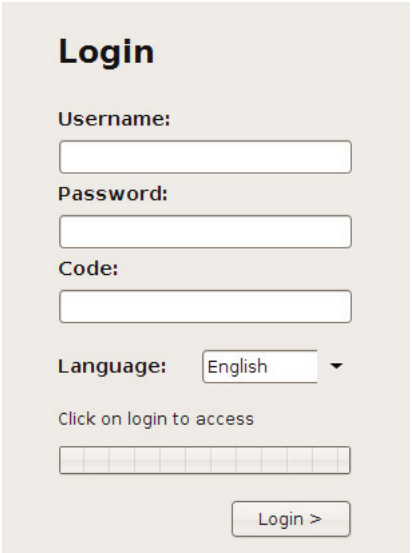
Option	Example		
Subject	SmartLiving control panel [Valid code]	Text, edited by the installer, associated with the respective event (in square brackets).	
Sender	SmartLAN@inim.biz	Parameters set by the installer	
Recipient	User1@inim.biz, User2@inim.biz		
Message text	---------- 01/01/2009 18:23:00 Valid code CODE 001 KEYP. 005 [PARTITION 001] ----------	The first part of the e-mail shows the date and time of the event (when saved to the events log) and any relative details.	
	Access with valid code entry saved to log.	Optional text Link to an internet website or IP address (if applicable).	
	http://www.inim.biz		
Attachment	map.pdf	Document/file sent with the e-mail	

Access the web-server 5-17-2

The security of the connection with the computer is guaranteed by integrated cryptography. The security of the connection of mobile-phone devices is guaranteed by the SSL protocol used for HTTPS connections.

Following is a description of the method of access to the interface which allows remote management of the control panel.

1. Type in the IP address on the navigation bar of the browser. If you wish to use HTTPS protocol, simply add the letter "s" to the "http" prefix (for example: "http://192.168.1.92" would become "https://192.168.1.92").
2. The control panel will open a page similar to the one opposite; type in "System user", "System password" (supplied by your installer) and your user code PIN.
   If you type the installer code, this will be accepted only if the Teleservice is enabled (paragraph *5-4 Activations*).
3. Press Login > to start the connection.



Please note that the SmartLAN/G board is capable of managing one connection at a time. Therefore, if another user is already connected to the control panel, access will be denied and the following message will be shown: "**Too many connections**".

Access will be denied in the following cases:

- the entered PIN is not recognized
- the entered PIN does not belong to any partition
- the entered PIN is not enabled
- the entered PIN is associated with a timer and the timer concerned is OFF.
- The "Internet Access" option from the Activations section in the User menu is disabled

If the connection is successful, the browser will show the first page of the web-server. The six icons listed below represent the six keys which allow the user to access the various sections:

Table 10: **Web-server sections**

Icon	Key	Note
	Accessing the virtual keypad	The keypad which is shown is the exact replica of the system keypad. Use Connect, to select another type of keypad (if required) from the top right section. At this point, use the virtual keypad in the same way as you would use the real one (access functions,etc.).
	Manage the partitions	The system will allow users to view only information relating to the partitions they control (refer to paragraph *5-2 Arming and disarming partitions*, paragraph *5-1 Managing alarms* and paragraph *5-5 View*).
	Manage zones and outputs	Using the mouse, select the desired partition. The system will show information regarding the zones belonging to the selected partition only and will allow you to inhibit/unbypass the zones as required (refer to paragraph *5-4 Activations* and paragraph *5-5 View*). The lower section allows you to view the current status of the outputs and activate/deactivate them as required (refer to paragraph *5-5 View* and paragraph *5-6 Activating/Deactivating outputs*).
	View timers	This section allows you to view the status of the 10 control panel timers (refer to paragraph *5-5 View*).
	View events log	Press Update Log to initialize and update the control panel events log (refer to paragraph *5-5 View*).
	End connection and exit	The control panel will end the connection and go back to the initial Log-in screen.

Mobile-phone web interface 5-17-3

The web-server interface for mobile-phone devices provides the same functions the user has access to when operating on the control panel from a remote computer.

To use this interface, you must connect to the SmartLAN address via a mobile phone (or similar device), the connection will be diverted automatically to the respective page. Otherwise, you can connect manually by adding "/mobile/" to the end of the SmartLAN/G address (e.g. "http://192.168.1.92" becomes "https://192.168.1.92/mobile/").

Once access to the web-server has been achieved, the cellphone display will show:

- the icons which access the various sections (top of display)
- the various objects available for selection (centre of display)
- the icons that represent the functions available for the selected objects (bottom of display).

All operations must be carried out as follows:

1. Select the desired section from those available at the top of display
2. Select the desired object, from those provided in the centre of display (: object selected, : object not selected)
3. Select the desired function, by means of the icons at the bottom of display (: function selected, : function not selected)
4. Press to send the command.
5. Press to update the display.

The difference between the web- interface and the computer interface is that mobile phone devices do not have access to a virtual keypad, however, they have two additional sections.

Table 11: **Web-server sections**

Icon	Key	Note
	Scenario activation	This section allows users to activate the scenarios they have access to (refer to paragraph *5-2 Arming and disarming partitions*).
	Outputs management	This section will allow users to view the status of the outputs and also activate/deactivate them (refer to paragraph *5-5 View* e paragraph *5-6 Activating/Deactivating outputs*)

Appendix A

TECHNICAL TERMINOLOGY AND GLOSSARY

ACCESS CODES

These are 4, 5 or 6 digit PINs which allow the building occupants (users) to access the system. Each code can be programmed to control specific functions only, and to operate the system to suit the requirements of the Main user.
Code types
- **Installer code**:used by the installer company technician
- **User code**:assigned to the building occupants

ALARM

Detection of non-authorized entry into the protected building. More specifically, activation of alarm signaling devices (detectors).

ALARM OR TAMPER MEMORY

In the event of:
- Zone Alarm
- terminal tamper
- open panel or dislodged panel
- peripheral tamper (keypads, expansions, readers)
- peripheral loss (keypads, expansions, readers)
- false key

The red LEDs on the system keypads and readers go On each time one of the previously-mentioned events occur. This visual warning signal is held even after the event ends (alarm memory), in order to warn you that an event occurred during your absence. This visual warning signal will be held until you clear the event memory (refer to Delete Memory).

ALARM RECEIVING CENTRE (ARC)

This is a private company that monitors premises protected by intrusion control systems equipped with Digital or Voice dialers (refer to Digital dialer and Voice dialer).
Alarm Receiving Centres receive alarm reports from monitored systems and take all the necessary actions to protect the occupants of the protected premises.

ANSWERPHONE

The "Answerphone" function, if enabled by the user, allows the control panel to answer incoming calls after a pre-set number of rings. The control panel will pick-up and play the recorded answer message.
During the call, the recipient can type-in a valid PIN (enabled for over-the-phone control) and access the authorized functions.

ARM/DISARM

User operations on one or more partitions. These generally indicate also the status of the partitions. Under normal circumstances, the zones of armed partitions can generate alarms. Under normal circumstances, the zones of disarmed partitions cannot generate alarms. The system generates tamper alarms even when partitions are disarmed.

AUTO-ARM

You can enable/disable the Auto-arm function on each separate partition.
If the auto-arm option is enabled on a timer-controlled partition, the partition will arm/disarm in accordance with the ON/OFF settings of the timer.

BACKUP BATTERY

This is the secondary power source of the system. If primary (230 Vac) power failure occurs, the battery will take over.

CALL QUEUE

A list of outgoing event-associated calls the control panel must send to programmed contact numbers.
Enabled users can clear the call queue manually.

DELAYED ENTRY ZONE

Violation of a zone with this configuration will not generate an alarm but will trigger the associated Timer (Entry time). If the user does not disarm the partition/s within the set "Entry time", the system will generate an alarm.
For example, the zone that monitors the main door of a building is usually configured as a Delayed Entry Zone, in order to give building occupants time to enter the building and disarm the partition without generating an alarm.

DELAYED EXIT ZONE

Violation of a zone with this configuration will not generate an alarm but will trigger the associated Timer (refer to Exit time).
For example, the zone that monitors the main door of a residence or building is usually configured as a delayed exit zone, in order to give occupants time to leave the partition after an arming operation. If the user does not leave the zone within the set "Exit time", the system will generate an alarm.

DELETE ALARM/ TAMPER MEMORY

This is an explicit user-command which ends signaling on the red keypad/reader LEDs of the following events:
- Zone Alarm
- terminal tamper
- open panel or dislodged panel
- peripheral tamper (keypads, expansions, readers)
- peripheral loss (keypads, expansions, readers)
- false key

If you delete the alarm/tamper memory, the visual signals on the red reader/keypad LEDs will clear.

DIGITAL DIALER

This device allows the control panel to send report calls to Alarm Receiving centres (ARC).
SmartLiving control panels provide a built-in digital dialer which supports all the most widely used protocols.

ENTRY TIME (OR ENTRY DELAY)

The time (expressed in minutes or seconds) that the system allows the user to disarm the partition after zone violation. It the system is not disarmed within the set time it will generate an alarm.
Each partition can be programmed with its own Entry time.

EVENT

An operative status recognized by the system.
For example: detector alarm, mains failure, user-code recognition, etc.
Each event (e.g. mains failure) can be associated with an activation event (when the event occurs) and a restoral event (when the event ends).
Each event can be programmed to generate the following actions:
- activation of one or more outputs
- transmission of one or more e-mails
- transmission of one or more SMS text messages
- activation of one or more voice calls
- activation of one or more digital calls

EVENTS LOG (OR EVENTS MEMORY)

This is the non-volatile portion of the memory the panels saves events to. The events are saved in chronological order with the following details:
- event description - with details regarding new events and restorals
- information regarding the user or the cause of event
- event location
- event date and time

The events log can be viewed by the system users and the installer.
Partition events (zone alarms, partition alarms, arm/disarm operations, recognized codes and keys, etc.) can be viewed by users with at least one partition in common with the event element.
For example, if a user arms several partitions from a keypad, the events log will show:
- description of the event - "Arm request"
- description of the code and partitions involved
- description (label) of the keypad involved
- date and time of the request

EXIT TIME (OR EXIT DELAY)

A short period (expressed in minutes or seconds) during which the user must disarm the partition after violation (for example, after opening the front door) otherwise the system will generate an alarm.
Each partition can be programmed with its own Exit time.

EXPANSION BOARDS (FLEX5)

These boards can be used to increase the number of terminals (zones or outputs) and/or the size of the system (in order to extend it over a larger partition). Expansion boards can be connected to the system via the I-BUS.

FAULT

A condition which indicates that a system component is not working properly.
Some faults can jeopardize the performance of the entire system. Mains failure (230V a.c.), telephone line-down and low battery are typical faults.

GSM DIALER

A device which allows the control panel to make telephone calls over the GSM network and also allows users to interact with the control panel over-the-phone or by means of SMS text messages.
The Nexus dialer is a peripheral device which is completely SmartLiving-system-integrated and is managed by the control panel BUS.
INIM's SmartLink is a similar device which is also compatible with control panels manufactured by other makers. This device is capable of providing the control panel with a telephone line even in the event of telephone line tamper (line cutting). This function increases the level of security considerably.

I-BUS

This is the two-way communication line (4 wires only) which connects the peripheral devices (keypads, readers, expansions, etc.) to the control panel.
The 4 easily identifiable wires, on the control panel motherboard and on the expansions, are:
- **"+"** power 12 Volt
- **"D"** data
- **"S"** data
- **"-"** Ground

INHIBITION - DEACTIVATION OF A ZONE

A disabled zone (inhibited) cannot generate alarms. Activation/Deactivation of zones can be carried out manually by users or, under certain circumstances, automatically by the control panel.

INSTALLER CODE

The Installer code is identified by a 4, 5 or 6 digit PIN. This PIN allows the installer to access the system Programming Menu either from a keypad or via the respective software application, on condition that all the system partitions are disarmed.

INSTALLER MENU

List of system functions and respective parameters accessed via keypad.
This menu allows the installer to program, check and change nearly all of the system parameters. The Installer Menu can be accessed from any keypad or via computer with the SmartLeague software, on condition that all the system partitions are disarmed.

INTERIOR ZONE

A zone that monitors the inside of the protected building.
For example, the interior zones of an office building are the zones that monitor offices and entrance points.
If a partition that a zone belongs to is armed in Stay mode, it will be unable to generate alarms.

KEY

A control device (card or keyfob) which allows the authorized user to access the system.
The key must be held in the vicinity of the reader in such a way to allow the system to read it and permit access to authorized operations.
Each key is programmed with:

- A random code selected from over 4 billion possible combinations.
- A label (usually the name of the user).
- The partitions it controls (arms, disarms, etc.).
- A group of pre-set parameters which allow the key user to operate the system in accordance with the authorized access level (for example, a key can be programmed to arm or disarm the system only at certain times of the day).

KEYPAD (JOY)

This device allows users to access and control the system. Keypads can be connected to the system via the I-BUS.
The keypad allows users to access and control the partitions which are common to both the code and keypad in use. The user can arm/disarm partitions, view the status of the zones, stop visual and audible signaling devices.

MAGNETIC CONTACT (AIR2-MC100)

A generic magnetic-contact is a detector/sensor based on an magnet which, when placed near the sensor, provokes the mechanical closure of an electrical contact.

OUTPUT

An electrical output point connected to a signaling or control device activated/deactivated by the control panel in response to programmed events.

PARTITION

A group of zones.
A partition identifies a group of zones that belong to a spatial or logical portion of the protected premises. For example, a partition may comprise all the zones that protect the downstairs partition of a house (spatial partition), or all the entrances of an office building (logical partition).

PARTITION ARM/ DISARM OPERATIONS

This refers to the status of a partition as requested by the user.
The user can carry out the following operations.

- **Disarm** - this operation disables the partition completely. In this way, none of the zones belonging to the partition can generate alarms.
- **Away mode** - this operation enables the interior and perimeter zones of the partition. In this way, all of the zones of the partition can generate alarms.
- **Stay mode -** this operation enables only the perimeter zones of the partition. In this way, only the perimeter zones of the partition can generate alarms.
- **Instant mode** - this operation enables the partition perimeter zones only and annuls delays. In this way, violation of the perimeter zones of the partition will generate instant alarms.
- **Hold** - this operation forces the partition to hold its current status.

PATROL

A periodic inspection of the protected premises carried out by authorized security staff.

PERIMETER ZONE

A zone that monitors the entrance points of the protected building.
Perimeter zones are usually direct entrance points such as doors and windows. For example, the front door of an apartment and windows that allow access from outside.

PERIPHERALS

Devices connected to the control panel via the I-BUS.
SmartLiving control panels manage the following peripherals:

- JOY series Keypads
- Proximity Readers (nBy)
- Expansions (Flex5)
- Transceiver (Air2-BS100)
- Sounder (Ivy)
- Isolators (IB100)
- GSM dialer (Nexus)

PRE-ARM TIME

The period (expressed in minutes) before an automatic arming operation.
For example, if a partition is set to arm automatically at 10:30 with a Pre-arm time of 5 minutes, all the partition keypads and readers will initiate an audible countdown at 10:25 in order to warn users of the forthcoming arming operation.
Each partition can be programmed with its own Pre-arm time.

PREMISES

The installation site.
Identifies the building or part protected by the intrusion control system, generally, a house or office.

PRIMARY POWER SOURCE

Under normal circumstances, the mains power supply (230Vac) 50 Hz (110V a.c. 60Hz in some countries).
Usually connected to a switching power supply or transformer (depending on the model) that provides the stabilized voltage to the system and the charge source to the batteries.

READER (NBY)

This device allows users to access and control the system. The system readers are connected to the control panel via the I-BUS.
The key (TAG) allows the user to activate shortcuts (refer to Shortcuts) and arm/disarm the partitions which are common to both the key (TAG) and reader in use. The key (TAG) must be held in the vicinity of the reader in such a way to allow the system to read it and permit access to authorized operations. Although readers provide a more limited access to the system, they are easiest way of carrying out day-to-day operations (arm, disarm, etc.).

SCENARIO

A pre-set arming configuration which applies various operating modes to the system partitions.

SHORTCUTS

The shortcuts allow quick access to User Menu options which normally require several step-by-step operations.

SUPERVISION

The "supervision time" is the interval during which the wireless-system devices (in general wireless detectors in permanent placements) must signal to the control panel that they are operating in the network. If a wireless device fails to signal before the "supervision time" expires, it will be classified as "Lost" and the control panel will trigger a "peripheral-loss" fault event.

TAMPER

Detection of a serious condition that jeopardizes the operating capacity of the device concerned and thus puts the system at risk.
Tamper conditions are detected by tamper switches connected to the system zones, keypads, readers, expansions and control panel. Generally, these events are triggered by system violation such as unauthorized opening of a keypad cover.

TELEPHONE ACTIONS

These are calls sent to programmed contact numbers when specific events start and end (restoral).

TELESERVICE

This is a service provided by the installer company. The installer company requires the user's collaboration and authorization before opening a teleservice session and working on the system via telephone line.

TEST ZONE

A zone with this attribute cannot generate alarms (activate audible and visual signaling devices). However, any alarm events that occur will be saved to the events memory.
If zones are not operating properly, the "Test" option will allow the installer to check them without the risk of generating false alarms

TIMER

A logical entity for automatic time-management of programmed peripherals or elements.
SmartLiving control panels provide 10 timers.

TRANSCEIVER

Transceiver-equipped devices
In two-way wireless systems, all the devices are equipped with transceivers. In one-way wireless systems, the main unit is equipped with a receiver module whereas the peripheral devices are equipped with transmitters.

USER CODE

Each code is programmed with:

- A 4, 5 or 6 digit PIN which allows access the system.
- A label which identifies the user (usually the user's name).
- The group of partitions it controls (arms, disarms, etc.).
- A group of pre-set parameters which allow the operator to work on the system in accordance with its authorized access level (for example, a code can be enabled to consult the events log but not to change the date and time).

USER MENU

List of functions available to the user after valid code entry at a keypad.

VOICE DIALER

This device allows the control panel to send voice calls to programmed contact numbers.
In SmartLiving control panels the voice dialer function is provided by the SmartLogos30M board (accessory item).

VOICE MEMO

If the system is equipped with a SmartLogos30M voice board, each JOY/MAX keypad, in the system configuration will allow users to record memos. Memos can be recorded, played, deleted as required.

WIRELESS

An intrusion control system whose devices (detectors, keypads, keyfobs) communicate with the control panel over radio waves.
Usually, only the control panel of wireless-systems is mains powered (220Va.c.) while, the wireless devices are battery powered. The battery life is of utmost importance in the design layout and operational capacity of these systems.

ZONE

An electrical input point used for the management/supervision of signals coming from an intrusion detection device.

Appendix B

SHORTCUTS AT DEFAULT

n.	ICON	description	function	parameter
1		**Arm/Disarm**	Applies a pre-set scenario	Scenario
2		**Stop alarms**	Immediately deactivates the outputs relative to zone/partition alarm and tamper events and system tamper events.	
3		**Clear call queue**	Cancels the call queue and stops ongoing calls (if any).	
4		**Delete memory**	Carries out a "Stop alarms" operation and, at the same time, deletes memory of system and partition alarm and tamper events.	
5		**Activate outputs**	Activates one of the programmed outputs.	Output
6		**Deactiv. outputs**	Deactivates one of the programmed outputs.	Output
7		**Overtime**	Delays auto-arming time of partitions by 30 minutes.	
8		**Teleservice req.**	Sends a call to the Installer company number (Teleservice number).	
9		**Voice menu**	Plays a recorded voice message which announces the shortcuts assigned to the number keys.	User code
10		**Listen-in**	Allows eavesdropping over-the-phone by means of a microphone located on suitably placed keypad.	Keypad
11		**Intercom Call**	Accesses the User Menu section: Voice functions/ Intercom Call	
12		**Arm/disarm menu**	Accesses the User Menu section: Arm/Disarm	
13		**Alarm menu**	Accesses the User Menu section: Manage alarms	
14		**Voice func. menu**	Accesses the User Menu section: Voice functions	
15		**Activations menu**	Accesses the User Menu section: Activations	
16		**View menu**	Accesses the User Menu section: View	
17		**Arming status**	Provides voice information regarding the armed/ disarmed status of the partitions.	
18		**Keypad sett.menu**	Accesses the User Menu section:Keypad Keypad	

n.	ICON	DESCRIPTION	function
19		**ZoneBypass menu**	Accesses the User Menu section: Activations/Zones
20		**Voice memo**	Accesses the User Menu section: Voice functions
21		**Output control**	Accesses the User Menu section: Outputs ON/OFF
22		**Enab.answerphone**	Accesses the User Menu section: Activations/ Answerphone
23		**Enab.teleservice**	Accesses the User Menu section: Activations/ Teleservice
24		**Enable codes**	Accesses the User Menu section: Activations/Codes
25		**Enable keys**	Accesses the User Menu section: Activations/Keys
26		**Enable timers**	Accesses the User Menu section: Activations/Timers
27		**Enab. auto-arm**	Accesses the User Menu section: Activations/Auto-arm
28		**View events log**	Accesses the User Menu section: View/Events log
29		**View alarm log**	Accesses the User Menu section: View/Alarms log
30		**View faults log**	Accesses the User Menu section: View/Faults log
31		**View arm ops log**	Accesses the User Menu section: View/Arm/Disarm op.
32		**ViewSystemStatus**	Accesses the User Menu section: View/System Voltage
33		**View zone status**	Accesses the User Menu section: View/Zone status
34		**Change PIN**	Accesses the User Menu section: Change PIN
35		**Time/Date**	Accesses the User Menu section: Time/Date
36		**View faults**	Accesses the User Menu section: View/Faults
37		**Thermostat**	Accesses the User Menu section:Thermostat

Appendix C

FAULT SIGNALS

The following table shows how system faults, indicated by the yellow LED, are signaled clearly on the keypad ⚠ :

FAULT	User menu string: "View/ Faults"	Probable cause	Note
Zone fuse blown	Zone fuse fault	Excessive current draw on the "+AUX" terminals on the control panel	
BUS fuse blown	IBUS fuse fault	Excessive current draw on the "+" terminal on the control panel	
Backup battery low or disconnected	Low battery	The control panel backup-battery is running low or is not connected properly	
Primary power source failure	Mains failure	The primary power source (230 Vac) has failed (blackout) or is not connected properly	
Telephone line down	Tel. line down	The telephone line is not working	
Wireless noise	Jamming	Rogue wireless signal	
Low wireless-detector battery	Low battery WLS	The battery of at least one wireless detector is running out	For information relating to "Low battery WLS" and "WLS zone loss" signaling, access the User menu, "View/Faults", press OK to view the list of devices involved
Wireless detector loss	WLS zone loss	At least one wireless detector is not responding (lost)	
Fault on Nexus GSM dialer	GSM fault / Low signal	The GSM network signal is insufficient	Press OK on "GSM fault" to access the list of current faults.
	GSM fault / GSM module fault	The GSM module of the Nexus dialer is not operating properly. Call your Installer company	
	GSM fault / SIM commun.fault	The SIM card does not respond or is not present. The SIM card PIN is not disabled.	
	GSM fault / Low credit	The remaining credit on the SIM card is below the minimum credit threshold.	
	GSM fault / Provider missing	The GSM network provider of the SIM in use is unavailable.	
Loss or tamper running	LossTamp.ongoing	One of the following events is present: • Panel open • Panel dislodged • Expansion tamper • Keypad tamper • Reader tamper • Sound.flash.Tamp • Expansion loss • Keypad loss • Reader loss • Sound.flash.Loss	
Faults on IVY-BUS sounderflasher	Sounder faults / Horn fault	A defect/damage has been detected on the horn/ sounder.	Press OK on "Sounder faults" to access the list of devices which have at least one fault present. Press OK on the selected sounderflasher to access the list of current faults on the device concerned.
	Sounder faults / LowBatt.Soundfl.	A low-voltage value has been detected on the sounderflasher battery. If the voltage drops below 10V, the device will inhibit the sounder and activate only the flasher (in the event of an alarm). If the voltage drops below 8V, the device will inhibit both the sounder and the flasher.	
	Sounder faults / Battery resist.	An excessive internal resistance has been detected on the sounderflasher battery. This type of deep fault indicates corrosion inside the battery, therefore, the battery must be replaced.	
Violation of zones with faults	Faults on zones	Violation has occurred on one or more zones with the "Fault zone" option enabled.	Press OK to access the list of zones involved.

DCMUINE0SLIVINGE-R400-20110121

Notes

ISO 9001:2008 Registered company

via Fosso Antico
Loc. Centobuchi
63076 Monteprandone
(AP) ITALY

Tel. +39 0735 705007
Fax +39 0735 704912

info@inim.biz
www.inim.biz